Docket No. 210580US2SRD

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Kenji OHKUMA, et al. GAU:

SERIAL NO: NEW APPLICATION EXAMINER:

FILED: HEREWITH

FOR: ENCRYPTION APPARATUS AND METHOD, AND DECRYPTION APPARATUS AND METHOD BASED ON BLOCK ENCRYPTION

REQUEST FOR PRIORITY

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

☐ Full benefit of the filing date of U.S. Application Serial Number, filed, is claimed pursuant to the provisions of **35 U.S.C. §120**.

☐ Full benefit of the filing date of U.S. Provisional Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §119(e)**.

■ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY	APPLICATION NUMBER	MONTH/DAY/YEAR
JAPAN	2000-198478	June 30, 2000

Certified copies of the corresponding Convention Application(s)

■ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

☐ were filed in prior application Serial No. filed

☐ were submitted to the International Bureau in PCT Application Number .
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

(B) Application Serial No.(s)

☐ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Marvin J. Spivak
Registration No. 24,913

C. Irvin McClelland
Registration Number 21,124

22850
Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 10/98)

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年　６月３０日

出願番号
Application Number: 特願２０００－１９８４７８

出願人
Applicant(s): 株式会社東芝

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年　５月３１日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号　出証特２００１－３０５０９３

【書類名】　特許願
【整理番号】　A000003588
【提出日】　平成12年 6月30日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 15/00
【発明の名称】　暗号化装置及び暗号化方法、復号装置及び復号方法並びに記録媒体
【請求項の数】　18
【発明者】
【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
【氏名】　大熊　建司
【発明者】
【住所又は居所】　東京都府中市東芝町１番地　株式会社東芝府中事業所内
【氏名】　佐野　文彦
【発明者】
【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
【氏名】　村谷　博文
【発明者】
【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
【氏名】　川村　信一
【特許出願人】
【識別番号】　000003078
【氏名又は名称】　株式会社　東芝
【代理人】
【識別番号】　100058479
【弁理士】

【氏名又は名称】　鈴江　武彦

【電話番号】　03-3502-3181

【選任した代理人】

【識別番号】　100084618

【弁理士】

【氏名又は名称】　村松　貞男

【選任した代理人】

【識別番号】　100068814

【弁理士】

【氏名又は名称】　坪井　淳

【選任した代理人】

【識別番号】　100092196

【弁理士】

【氏名又は名称】　橋本　良郎

【選任した代理人】

【識別番号】　100091351

【弁理士】

【氏名又は名称】　河野　哲

【選任した代理人】

【識別番号】　100088683

【弁理士】

【氏名又は名称】　中村　誠

【選任した代理人】

【識別番号】　100070437

【弁理士】

【氏名又は名称】　河井　将次

【手数料の表示】

【予納台帳番号】　011567

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　暗号化装置及び暗号化方法、復号装置及び復号方法並びに記録媒体

【特許請求の範囲】

【請求項１】

ブロック暗号方式による暗号化装置であって、

ブロックデータに対してそれを複数に分割した部分データごとに局所的な拡散を行う機能を含む第１の処理手段と、

前段の前記第１の処理手段から出力されるブロックデータに対してそのブロック幅にわたる線形拡散処理を行って後段の前記第１の処理手段へ入力する機能を含む第２の処理手段とを備え、

前記第２の処理手段は、前段の前記第１の処理手段に対する入力ブロックデータにおける少なくとも１つの特定ビットの状態を、後段の前記第１の処理手段に対する入力ブロックデータにおける少なくとも１つの特定ビットへ、複数の演算経路を辿って波及させるための手段を含むものであることを特徴とする暗号化装置。

【請求項２】

前記特定ビットは、各々の前記入力部分データに少なくとも１つずつ存在することを特徴とする請求項１に記載の暗号化装置。

【請求項３】

前記第２の処理手段は、前段の前記第１の処理手段に対する入力ブロックデータから選択した１ビットと、後段の前記第１の処理手段に対する入力ブロックデータから選択した１ビットとからなる全ての組み合わせ又はそのうちで所定の条件を満たす複数の組み合わせの各々について、前段側における当該１ビットの状態を、後段側における当該１ビットへ、複数の演算経路を辿って波及させるための手段を含むものであることを特徴とする請求項１に記載の暗号化装置。

【請求項４】

ブロック暗号方式による暗号化装置であって、

ブロックデータを複数に分割した各分割部分データに対してそれぞれ非線形変

換処理を施す並列させた複数の第１の非線形変換処理手段の一群と、ブロックデータのブロック幅にわたる線形拡散処理を施す第１の線形拡散処理手段とを備え、

前記第１の非線形変換処理手段は、前記部分データのデータ幅をさらに複数に分割した各再分割部分データに対してそれぞれ非線形変換処理を施す並列させた複数の第２の非線形変換処理手段の一群と、前記部分データのデータ幅にわたる線形拡散処理を施す第２の線形拡散処理手段とを含むものであり、

前記第１の線形拡散処理手段は、前段の複数の第１の非線形変換処理手段の各々の最終段に並列させた複数の第２の非線形変換処理手段の各々から出力される全再分割部分データからなるブロックデータに線形拡散処理を施して後段の複数の第１の非線形変換処理手段の各々の初段に並列させた複数の第２の非線形変換処理手段の一群の各々へ各再分割部分データとして入力するものであるとともに、後段の複数の第１の非線形変換処理手段の初段の複数の第２の非線形変換処理手段への入力となる複数の再分割部分データのうちの少なくとも１つを、前段のいずれか同一の第１の非線形変換処理手段の最終段の複数の第２の非線形変換処理手段から出力される複数の再分割部分データのうちの少なくとも２つに基づいて求めることを特徴とする暗号化装置。

【請求項５】

前記第１の線形拡散処理手段は、後段の全第１の非線形変換処理手段の各々について、当該後段の第１の非線形変換処理手段の初段の複数の第２の非線形変換処理手段への入力となる複数の再分割部分データのうちの少なくとも１つを、前段の各第１の非線形変換処理手段ごとにその最終段の複数の第２の非線形変換処理手段から出力される複数の再分割部分データのうちから少なくとも２つずつ選択された再分割部分データ群に基づいて求めることを特徴とする請求項４に記載の暗号化装置。

【請求項６】

前記第１の線形拡散処理手段は、後段の各第１の非線形変換処理手段の初段の各第２の非線形変換処理手段への入力となる各再分割部分データを、それぞれ、前段の各第１の非線形変換処理手段ごとにその最終段の複数の第２の非線形変換

処理手段から出力される複数の再分割部分データのうちから少なくとも２つずつ選択された再分割部分データ群に基づいて求めることを特徴とする請求項５に記載の暗号化装置。

【請求項７】

前記分割部分データはすべて同一ビット長であるとともに、前記再分割部分データはすべて同一ビット長であり、

前記第１の線形拡散処理手段は、各々の前記再分割部分データから相対応する１ビットずつを取りだしたビット群に対して施す線形拡散処理を、該１ビットを取り出す位置を排他的に変えたものについてそれぞれ行うことによって、ブロックデータのブロック幅にわたる線形拡散処理を行うものであることを特徴とする請求項５または６に記載の暗号化装置。

【請求項８】

前記ブロックデータは１２８ビットであり、前記分割部分データは３２ビットであり、前記再分割部分データは８ビットであり、

前記第１の線形拡散処理手段は、１６個の前記再分割部分データの各々から同一位置の１ビットずつを取りだして得た１６ビットデータに対して施す線形拡散処理を、該１ビットを取り出す位置を排他的に変えた８つの１６ビットデータのそれぞれについて行うものであることを特徴とする請求項７に記載の暗号化装置。

【請求項９】

前記第１の線形拡散処理手段は、実回路によって実装されたものであることを特徴とする請求項５ないし８のいずれか１項に記載の暗号化装置。

【請求項１０】

前記第１の線形拡散処理手段の入力側のビットと出力側のビットとの間の結合関係は、ガロア体の乗算に基づいて決定されたものであることを特徴とする請求項９に記載の暗号化装置。

【請求項１１】

前記第１の線形拡散処理手段は、ソフトウェアを実行することによって実現されるものであることを特徴とする請求項５ないし８のいずれか１項に記載の暗号

化装置。

【請求項１２】

共通鍵ブロック暗号方式による暗号化装置であって、

初段では入力された１２８ビットの平文ブロックデータを、２段目以降では前段での処理が施された１２８ビットのブロックデータを入力とし、該ブロックデータを４分割した４組の３２ビット・データに対してそれぞれ局所的な線形拡散処理および非線形変換処理を施し出力する４つの第１の非線形変換処理部と、これら４つの第１の非線形変換処理部からそれぞれ出力された４組の３２ビット・データを連結した１２８ビットのブロックデータに対して最大距離分離行列を用いて線形拡散処理を施し次段へ出力する第１の拡散処理部とを、１段分の段構成として、該段構成を所定段数分接続し、

最後の前記第１の拡散処理部の後段に、この第１の拡散処理部から出力される１２８ビットのブロックデータを入力とする前記４つの第１の非線形変換処理部を接続し、

この４つの第１の非線形変換処理部の後段に、これら４つの第１の非線形変換処理部からそれぞれ出力された４組の３２ビット・データを連結した１２８ビットのブロックデータに対して１２８ビットの鍵データを加算して１２８ビットの暗号化されたブロックデータとして出力する第１の鍵加算部を接続して構成されるとともに、

前記第１の非線形変換処理部の各々は、与えられた１組の前記３２ビット・データをさらに４分割した４組の８ビット・データに対してそれぞれ８ビットの鍵データを加算する４つの第２の鍵加算部と、各第２の鍵加算部の出力に対してそれぞれ８ビットの入出力変換表を用いて非線形変換を行う４つの第２の非線形変換処理部と、これら４つの第２の非線形変換処理部からそれぞれ出力された４組の８ビット・データを連結した３２ビット・データに対して最大距離分離行列を用いて線形拡散処理を施す第２の拡散処理部と、この第２の拡散処理部の後段にさらに接続された４組の前記第２の鍵加算部および第２の非線形変換処理部とを含むものであり、

前記第１の拡散処理部の各々は、前段の１つの第１の非線形変換処理部の４つ

の第２の非線形変換処理部からそれぞれ出力される８ビットのうちの相対応する１ビットを一纏めにした４ビットを行列演算における入力側の１つの要素とするとともに、後段の１つの第１の非線形変換処理部の４つの第２の非線形変換処理部へそれぞれ入力される８ビットのうちの相対応する１ビットを一纏めにした４ビットを行列演算における出力側の１つの要素として、2^4のガロア体の乗算に基づいた４行４列の行列演算またはこれと等価な回路によって線形拡散処理を行う１６ビット拡散手段を、該前段及び後段の第２の非線形変換処理部についての該８ビットのうちの各ビットに対応して有し、

１つの前記１６ビット拡散手段における前記2^4のガロア体の乗算に基づいた４行４列の行列演算またはこれと等価な回路では、前段の４つの第１の非線形変換処理手段の最終段における合計１６の第２の非線形変換処理手段からの出力となる任意の１ビットと、後段の４つの第１の非線形変換処理手段の初段における合計１６の第２の非線形変換処理手段へ入力となる任意の１ビットとのすべての組み合わせにおいて、前段側における当該１ビットの状態を、後段側における当該１ビットへ、複数の演算経路を辿って波及させるための手段を含むものであることを特徴とする暗号化装置。

【請求項１３】

共通鍵ブロック暗号方式による暗号化装置であって、

初段では入力された６４ビットの平文ブロックデータを、２段目以降では前段での処理が施された６４ビットのブロックデータを入力とし、該ブロックデータを２分割した２組の３２ビット・データに対してそれぞれ局所的な線形拡散処理および非線形変換処理を施し出力する２つの第１の非線形変換処理部と、これら２つの第１の非線形変換処理部からそれぞれ出力された２組の３２ビット・データを連結した６４ビットのブロックデータに対して最大距離分離行列を用いて線形拡散処理を施し次段へ出力する第１の拡散処理部とを、１段分の段構成として、該段構成を所定段数分接続し、

最後の前記第１の拡散処理部の後段に、この第１の拡散処理部から出力される６４ビットのブロックデータを入力とする前記２つの第１の非線形変換処理部を接続し、

この２つの第１の非線形変換処理部の後段に、これら２つの第１の非線形変換処理部からそれぞれ出力された２組の３２ビット・データを連結した６４ビットのブロックデータに対して６４ビットの鍵データを加算して６４ビットの暗号化されたブロックデータとして出力する第１の鍵加算部を接続して構成されるとともに、

前記第１の非線形変換処理部の各々は、与えられた１組の前記３２ビット・データをさらに４分割した４組の８ビット・データに対してそれぞれ８ビットの鍵データを加算する４つの第２の鍵加算部と、各第２の鍵加算部の出力に対してそれぞれ８ビットの入出力変換表を用いて非線形変換を行う４つの第２の非線形変換処理部と、これら４つの第２の非線形変換処理部からそれぞれ出力された４組の８ビット・データを連結した３２ビット・データに対して最大距離分離行列を用いて線形拡散処理を施す第２の拡散処理部と、この第２の拡散処理部の後段にさらに接続された４組の前記第２の鍵加算部および第２の非線形変換処理部とを含むものであり、

前記第１の拡散処理部の各々は、前段の１つの第１の非線形変換処理部の４つの第２の非線形変換処理部からそれぞれ出力される８ビットのうちの相対応する１ビットを一纏めにした４ビットを行列演算における入力側の１つの要素とするとともに、後段の１つの第１の非線形変換処理部の４つの第２の非線形変換処理部へそれぞれ入力される８ビットのうちの相対応する１ビットを一纏めにした４ビットを行列演算における出力側の１つの要素として、2^4のガロア体の乗算に基づいた２行２列の行列演算またはこれと等価な回路によって線形拡散処理を行う８ビット拡散手段を、該前段及び後段の第２の非線形変換処理部についての該８ビットのうちの各ビットに対応して有し、

１つの前記８ビット拡散手段における前記2^4のガロア体の乗算に基づいた２行２列の行列演算またはこれと等価な回路では、前段の２つの第１の非線形変換処理手段の最終段における合計８の第２の非線形変換処理手段からの出力となる任意の１ビットと、後段の２つの第１の非線形変換処理手段の初段における合計８の第２の非線形変換処理手段へ入力となる任意の１ビットとのすべての組み合わせにおいて、前段側における当該１ビットの状態を、後段側における当該１ビ

ットへ、複数の演算経路を辿って波及させるための手段を含むものであることを特徴とする暗号化装置。

【請求項１４】

ブロック暗号方式による暗号化方法であって、

ブロックデータに対してそれを複数に分割した部分データごとに局所的な拡散を行う機能を含む第１の処理と、

前段の前記第１の処理手段から出力されるブロックデータに対してそのブロック幅にわたる線形拡散処理を行って後段の前記第１の処理手段へ入力する機能を含む第２の処理とを実行するステップを有し、

前記第２の処理は、前段の前記第１の処理手段に対する入力ブロックデータにおける少なくとも１つの特定ビットの状態を、後段の前記第１の処理手段に対する入力ブロックデータにおける少なくとも１つの特定ビットへ、複数の演算経路を辿って波及させるための機能を含むものであることを特徴とする暗号化方法。

【請求項１５】

ブロック暗号方式による暗号化プログラムを記録したコンピュータ読取り可能な記録媒体において、

ブロックデータに対してそれを複数に分割した部分データごとに局所的な拡散を行う機能を含む第１の処理機能と、

前段の前記第１の処理手段から出力されるブロックデータに対してそのブロック幅にわたる線形拡散処理を行って後段の前記第１の処理手段へ入力する機能を含む第２の処理機能であって、前段の第１の処理手段に対する入力ブロックデータにおける少なくとも１つの特定ビットの状態を、後段の第１の処理手段に対する入力ブロックデータにおける少なくとも１つの特定ビットへ、複数の演算経路を辿って波及させるための機能を含む第２の処理機能とを、コンピュータに実現させるためのプログラムを記録したコンピュータ読取り可能な記録媒体。

【請求項１６】

ブロック暗号方式による復号装置であって、

ブロックデータに対してそれを複数に分割した部分データごとに局所的な拡散を行う機能を含む第１の処理手段と、

前段の前記第１の処理手段から出力されるブロックデータに対してそのブロック幅にわたる線形拡散処理を行って後段の前記第１の処理手段へ入力する機能を含む第２の処理手段とを備え、

前記第２の処理手段は、前段の前記第１の処理手段に対する入力ブロックデータにおける少なくとも１つの特定ビットの状態を、後段の前記第１の処理手段に対する入力ブロックデータにおける少なくとも１つの特定ビットへ、複数の演算経路を辿って波及させるための手段を含むものであることを特徴とする復号装置。

【請求項１７】

ブロック暗号方式による復号方法であって、

ブロックデータに対してそれを複数に分割した部分データごとに局所的な拡散を行う機能を含む第１の処理と、

前段の前記第１の処理手段から出力されるブロックデータに対してそのブロック幅にわたる線形拡散処理を行って後段の前記第１の処理手段へ入力する機能を含む第２の処理とを実行するステップを有し、

前記第２の処理は、前段の前記第１の処理手段に対する入力ブロックデータにおける少なくとも１つの特定ビットの状態を、後段の前記第１の処理手段に対する入力ブロックデータにおける少なくとも１つの特定ビットへ、複数の演算経路を辿って波及させるための機能を含むものであることを特徴とする復号方法。

【請求項１８】

ブロック暗号方式による復号プログラムを記録したコンピュータ読取り可能な記録媒体において、

ブロックデータに対してそれを複数に分割した部分データごとに局所的な拡散を行う機能を含む第１の処理機能と、

前段の前記第１の処理手段から出力されるブロックデータに対してそのブロック幅にわたる線形拡散処理を行って後段の前記第１の処理手段へ入力する機能を含む第２の処理機能であって、前段の第１の処理手段に対する入力ブロックデータにおける少なくとも１つの特定ビットの状態を、後段の第１の処理手段に対する入力ブロックデータにおける少なくとも１つの特定ビットへ、複数の演算経路

を辿って波及させるための機能を含む第２の処理機能とを、コンピュータに実現させるためのプログラムを記録したコンピュータ読取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ブロック暗号方式による暗号化装置及び暗号化方法並びに復号装置及び復号方法に関する。

【０００２】

【従来の技術】

共通鍵ブロック暗号の代表的な基本構造にＳＰＮ型とＦｅｉｓｔｅｌ型があり、各々について差分／線形解読法に対する強度評価と耐性を高める設計法が研究されている（文献[１]V.Rijmen, J.Daemen, B.Preneel, A.Bosselaers, E.DcWin, “The Cipher SHARK,” Fast Software Encryption, LNCS 1039,1996.、文献[２]青木和麻呂,太田和夫,“最大平均差分確率および最大平均線形確率のより厳密な評価,” SCIS 96-4A,1996.、文献[３]松井充,“ﾌﾞﾛｯｸ暗号MISTY,” ISEC 96-11,1996.）。ＳＰＮ構造では、活性Ｓ－ｂｏｘ数の保証が出来るので、設定した強度を達成するための段数決定がしやすい（文献[１]）。しかし、ブロック・サイズが大きくなりＳ－ｂｏｘの並列度が上がると、拡散層の処理が複雑になり、速度が低下する傾向がある。

【０００３】

この点を改善したのが、ＳＱＵＡＲＥ／Ｒｉｊｎｄａｅｌ型の暗号である（文献[４]J.Daemen, L.R.Knudsen, V.Rijmen, “The Block Cipher Square,” Fast Software Encryption, LNCS 1267,1997.、文献[５]J.Daemen, V.Rijmen, “AES Proposal: Rijndael,” http://www.east.kuleuven.ac.be/~rijmen/rijdael/rijndaeldocV2.zip）。この型の暗号では、１６個の並列Ｓ－ｂｏｘを４×４の行列状に並べて線形拡散を同一列内に制限することで処理を軽減している。また、線形拡散にバイト位置の並べ替えを組み合わせることで、ある段の１バイトの影響は２段後に全バイトに広がり、４段で活性Ｓ－ｂｏｘ数は２５以上を達成している。

【０００４】

しかしながら、同一列内のバイトが次の段で混合しないという性質があるため、ＳＱＵＡＲＥ攻撃という専用の攻撃法が存在する（文献[１]、文献[５]）。これは、拡散層が１種類という制約下で、強度と効率の両立を目指した結果と考えることが出来る。

【０００５】

【発明が解決しようとする課題】

ＳＰＮ型構造は、活性Ｓ－ｂｏｘ数の下限の見積もりが容易で、差分／線形解読法に対する強度を保証した設計が可能である。しかしながら、平文／暗号文のブロック・サイズの増加に従い、Ｓ－ｂｏｘの並列度が高くなると、拡散層の結合部の計算コストも高くなるという欠点があった。また、拡散層の設計によってデータ攪拌が均一でなくなる可能性があった。

【０００６】

本発明は、上記事情を考慮してなされたもので、計算コストを抑えたまま高く均一な拡散を可能とする暗号化装置及び暗号化方法並びに復号装置及び復号方法を提供することを目的とする。

【０００７】

【課題を解決するための手段】

本発明は、ブロック暗号方式による暗号化装置であって、ブロックデータに対してそれを複数に分割した部分データごとに局所的な拡散を行う機能を含む第１の処理手段と、前段の前記第１の処理手段から出力されるブロックデータに対してそのブロック幅にわたる線形拡散処理を行って後段の前記第１の処理手段へ入力する機能を含む第２の処理手段とを備え、前記第２の処理手段は、前段の前記第１の処理手段に対する入力ブロックデータにおける少なくとも１つの特定ビットの状態を、後段の前記第１の処理手段に対する入力ブロックデータにおける少なくとも１つの特定ビットへ、複数の演算経路を辿って波及させるための手段を含むものであることを特徴とする。

好ましくは、前記特定ビットは、各々の前記入力部分データに少なくとも１つずつ存在するようにしてもよい。

好ましくは、前記第２の処理手段は、前段の前記第１の処理手段に対する入力ブロックデータから選択した１ビットと、後段の前記第１の処理手段に対する入力ブロックデータから選択した１ビットとからなる全ての組み合わせ又はそのうちで所定の条件を満たす複数の組み合わせの各々について、前段側における当該１ビットの状態を、後段側における当該１ビットへ、複数の演算経路を辿って波及させるための手段を含むものであるようにしてもよい。

【０００８】

また、本発明は、ブロック暗号方式による暗号化装置であって、ブロックデータを複数に分割した各分割部分データに対してそれぞれ非線形変換処理を施す並列させた複数の第１の非線形変換処理手段の一群と、ブロックデータのブロック幅にわたる線形拡散処理を施す第１の線形拡散処理手段とを備え、前記第１の非線形変換処理手段は、前記部分データのデータ幅をさらに複数に分割した各再分割部分データに対してそれぞれ非線形変換処理を施す並列させた複数の第２の非線形変換処理手段の一群と、前記部分データのデータ幅にわたる線形拡散処理を施す第２の線形拡散処理手段とを含むものであり、前記第１の線形拡散処理手段は、前段の複数の第１の非線形変換処理手段の各々の最終段に並列させた複数の第２の非線形変換処理手段の各々から出力される全再分割部分データからなるブロックデータに線形拡散処理を施して後段の複数の第１の非線形変換処理手段の各々の初段に並列させた複数の第２の非線形変換処理手段の一群の各々へ各再分割部分データとして入力するものであるとともに、後段の複数の第１の非線形変換処理手段の初段の複数の第２の非線形変換処理手段への入力となる複数の再分割部分データのうちの少なくとも１つを、前段のいずれか同一の第１の非線形変換処理手段の最終段の複数の第２の非線形変換処理手段から出力される複数の再分割部分データのうちの少なくとも２つに基づいて求めることを特徴とする。

好ましくは、前記第１の線形拡散処理手段は、後段の全第１の非線形変換処理手段の各々について、当該後段の第１の非線形変換処理手段の初段の複数の第２の非線形変換処理手段への入力となる複数の再分割部分データのうちの少なくとも１つを、前段の各第１の非線形変換処理手段ごとにその最終段の複数の第２の非線形変換処理手段から出力される複数の再分割部分データのうちから少なくと

も２つずつ選択された再分割部分データ群に基づいて求めるようにしてもよい。

好ましくは、前記第１の線形拡散処理手段は、後段の各第１の非線形変換処理手段の初段の各第２の非線形変換処理手段への入力となる各再分割部分データを、それぞれ、前段の各第１の非線形変換処理手段ごとにその最終段の複数の第２の非線形変換処理手段から出力される複数の再分割部分データのうちから少なくとも２つずつ選択された再分割部分データ群に基づいて求めるようにしてもよい。

【０００９】

なお、暗号化装置に係る本発明は、暗号方法に係る発明、復号装置に係る発明、復号方法に係る発明としても成立する（もちろん、従属項についても同様である）。

また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【００１０】

本発明では、局所的なデータ拡散を行う小型の拡散層とブロック幅に及ぶ拡散を行う大型の拡散層を交互に重ねて運用する。本発明によれば、複数種類の異なる拡散（例えば、大小２段階の拡散）によって、計算コストを抑えたまま高く均一な拡散を実現した。また、階層的にブランチ数が保証でき（ブランチ数の階層性）、活性Ｓ－ｂｏｘ数の下限を容易に保証できる。また、強度評価がしやすいという特性がある。

【００１１】

ＳＱＵＡＲＥ暗号やＲｉｊｎｄａｅｌ暗号では、小型の拡散とバイト単位の並べ方によって同等の効果を実現している。しかし、それらの暗号では拡散層が１種類であるため、ＳＱＵＡＲＥ攻撃と呼ばれる解読法が存在する。本発明では、大小２種類の拡散層の組み合わせ方によって、ＳＱＵＡＲＥ攻撃に対する耐性の

向上が可能である。

【００１２】

また、大型の拡散層の構造を工夫することによって、例えば、その前段のＳ－ｂｏｘと後段のＳ－ｂｏｘとの間の組み合わせの全部または一部について、差分経路を複線化することによって、高いなだれ効果が得られ、より効果的なＳＱＵＡＲＥ攻撃に対する耐性の向上が可能になる。

【００１３】

【発明の実施の形態】

以下、図面を参照しながら発明の実施の形態を説明する。

【００１４】

本実施形態では、局所的な拡散（小拡散）と、ブロック幅に渡る拡散（大拡散）との組み合わせによる、入れ子型（再帰的）ＳＰＮ構造の暗号方式について説明する。

【００１５】

以下では、暗号化を中心に説明し、その後で復号について説明する。なお、復号アルゴリズムは、暗号アルゴリズムの逆変換であり、鍵は暗号化と復号で共通の、秘密の鍵である。

【００１６】

また、本暗号方式は、ハードウェアによってもソフトウェアによっても実現可能であり、以下に示す構成例は、暗号化装置（復号装置）の機能ブロック図としても成立し、また暗号アルゴリズム（復号アルゴリズム）の機能モジュール図としても成立する。

【００１７】

図１に、入れ子型（再帰的）ＳＰＮ構造の暗号方式（暗号化装置（もしくは復号装置）または暗号アルゴリズム（もしくは復号アルゴリズム）、暗号処理装置）の基本的な構成例を示す。

【００１８】

図１に示されるように、入れ子型ＳＰＮ構造では、各段において複数並列に並んだ非線形変換モジュール（後述の例では拡大Ｓ－ｂｏｘ）２の各々により局所

的な小拡散を行い、次いで拡散モジュール（後述の例では大ＭＤＳ）３によりブロック幅に渡る大拡散を行い、また非線形変換モジュール２により局所的な小拡散を行い、ということを所定段数繰り返す。さらに、非線形変換モジュール２は、非線形変換モジュール（後述の例ではＳ－ｂｏｘ）４と拡散モジュール（後述の例では小ＭＤＳ）５とを交互に配列して構成される。

【００１９】

すなわち、本実施形態の入れ子型ＳＰＮ構造は、通常のＳＰＮ構造のＳ－ｂｏｘの部分に小型のＳＰＮ構造（後述の例では２段のＳＰＮ構造）を再帰的に埋め込んだものである。

【００２０】

このような入れ子型ＳＰＮ構造によれば、ブランチ数が階層的に保証でき（ブランチ数の階層性）、活性Ｓ－ｂｏｘ数の下限を容易に保証できる、という優れた特質が得られる。また、入れ子型ＳＰＮ構造には、この他に、単純明快な構造のため、強度評価がしやすいという特性がある。

【００２１】

なお、図１では、局所的な小拡散を４並列で表しているが、これに限定されるものではなく、それ以外の並列数も可能である。

また、図１では、全ブロック長を均等に分割した複数の小拡散を並列されているが、これに限定されるものではなく、異なるビット長の小拡散を複数組み合わせることも可能である。また、この場合に、全ての小拡散のビット長を異なるようにしてもよいし、一部の小拡散のビット長は同じであってもよい。

また、図１では、１種類の局所的な小拡散を用いているが、２種類以上の局所的な小拡散を用いることも可能である（例えば、図１において、ブロック幅に渡る拡散モジュール３を、１つおきに、２つの非線形変換モジュール２に渡る拡散モジュールに替えた構成）。

また、同一構成の繰り返し構造にする方法の他に、一部のみ構成を替えることも可能である。

また、例えば、全ての非線形変換モジュール２の構成を同一構成にすることも、非線形変換モジュール２について、異なる構成を混在させることも可能である

。この点は、拡散モジュール３、非線形変換モジュール４、拡散モジュール５のそれぞれについても同様である。

また、例えば、最初の入力段と、最後の出力段だけ、他の中間段とは異なる内部構成にしてもよい。

また、図１では、２階層の入れ子構造であるが、３階層以上の入れ子構造も可能である（３階層の場合、例えば、非線形変換モジュール４をさらにＳＰＮ構造にする）。また、例えば、非線形変換モジュール２によって階層構造を異ならせることも可能である。

この他にも、種々のバリエーションが考えられる。

【００２２】

以下では、８ビットＳ－ｂｏｘを利用したＡＥＳ相当の１２８ビット・ブロック暗号の具体例を用いつつ本実施形態について説明する。

【００２３】

ここで、ブロック暗号の強度評価に関して説明する。

【００２４】

与えられた関数ｆの暗号強度を見積もる重要な指標として最大差分確率／最大線形確率がある。

【００２５】

［最大差分確率、最大線形確率の定義］

関数ｆ（ｘ）に対し、最大差分確率ｄｐ^{f}と最大線形確率ｌｐ^{f}はそれぞれ次式で表される。

【００２６】

【数１】

$$dp^{f} \equiv \max_{\Delta x \neq 0, \Delta y} \left| \frac{\#\{x \mid f(x) \oplus f(x \oplus \Delta x) = \Delta y\}}{2^{n}} \right|$$

$$lp^{f} \equiv \max_{\Gamma x, \Gamma y \neq 0} \left| 2\frac{\#\{x \mid x \cdot \Gamma x = f(x) \cdot \Gamma y\}}{2^{n}} - 1 \right|$$

【００２７】

ここで、Δｘはｘの入力差分、Γｘはｘのマスク値を表す。

【００２８】

一般には、最大差分確率ｄｐ^{f}や最大線形確率ｌｐ^{f}を求めることが困難な場合が多い。ここで、その近似値として最大差分特性確率ＤＰ^{f}および最大線形特性確率ＬＰ^{f}で安全性を評価する。

【００２９】

本実施形態では、入れ子型ＳＰＮ構造を暗号化関数として用いる。ここでは、その基本構造であるＳＰＳ構造の特性について述べる。ここで、ＳＰＳとは、Ｓ－ｂｏｘ層と拡散層ＰをＳ－Ｐ－Ｓのように３層重ねた構造を指す。

【００３０】

［ブランチ数］

ＳＰＳ構造において入力ｘに対する拡散層の出力がθ（ｘ）のとき、差分解読に対するブランチ数Ｂは次式で定義する（文献［１］、文献［６］清水秀夫，金子敏信，“共通鍵暗号のdiffusion層について，”SCIS 99-72,1999.）。

【００３１】

【数２】

$$B \equiv \min_{\Delta x \neq 0}(w(\Delta x) + w(\theta(\Delta x)))$$

【００３２】

ここで、ｗ（）はＳ－ｂｏｘのビット幅を符号長としたハミング距離である。非零の入出力差分に接続するＳ－ｂｏｘを活性Ｓ－ｂｏｘと呼ぶ。

【００３３】

この拡散層の入出力にＳ－ｂｏｘを接続した構造をＳＰＳ構造と呼ぶ。Ｓ－ｂｏｘが全単射のとき、ＳＰＳ構造への入力ビットに非零の差分を持つものが１個でもあれば、ブランチ数の定義により、活性Ｓ－ｂｏｘはブランチ数以上（すなわちＢ以上）になる。また、Ｓ－ｂｏｘの最大差分確率をp_sとすると、ＳＰＳ構造の最大差分特性確率は、上界値p_s^{B}を越えない。

【００３４】

［ＭＤＳ（Ｍａｘｉｍｕｍ　Ｄｉｓｔａｎｃｅ　Ｓｅｐａｒａｂｌｅ）行列］

ＳＰＳ構造のＳ層としてM並列のＳ－ｂｏｘを用いた場合、それらを結合する拡散層のブランチ数は（Ｍ＋１）以下であり、ブランチ数が（Ｍ＋１）を満たす線形変換をＭＤＳ（Ｍａｘｉｍｕｍ　Ｄｉｓｔａｎｃｅ　Ｓｅｐａｒａｂｌｅ；最大距離分離）行列と呼ぶ。

【００３５】

拡散層がＭＤＳ行列であるとき、ＳＰＳ構造の最大差分特性確率は上界値p_s^{M+1}を越えない［１］。同様に、Ｓ－ｂｏｘの最大線形確率をq_sとすると、ＳＰＳ構造の最大線形特性確率はq_s^{M+1}を越えない。

【００３６】

［入れ子型ＳＰＳ構造のブランチ数］

２段ＳＰＮ構造をそれより大きなＳＰＮ構造のＳ－ｂｏｘとして利用するとき、拡大Ｓ－ｂｏｘ（小構造）と呼ぶことにする。ここで、Ｓ－ｂｏｘはM_1並列であり、拡大Ｓ－ｂｏｘ内の拡散層のブランチ数をB_1とする。拡大Ｓ－ｂｏｘに対するM_2並列の２段ＳＰＮ構造（大構造）を考え、その拡散層のブランチ数をB_2とする。このとき、大構造中の活性Ｓ－ｂｏｘ数は下界値$B_1 \cdot B_2$を下回らない。この性質がブランチ数の階層性である。

【００３７】

また、大小２種類の拡散層の両方がＭＤＳ行列であるとき、活性Ｓ－ｂｏｘ数は$(M_1+1)(M_2+1)$を下回らない。これにより、入れ子型ＳＰＮ構造のDP^f、LP^fの上限を抑えることが可能になる。

【００３８】

図２に、$M_1=M_2=4$の場合の例を示す。１５が後述する大ＭＤＳ行列による拡散部を示し、１１～１４がその入力側の拡大Ｓ－ｂｏｘを示し、１６～１９がその出力側の拡大Ｓ－ｂｏｘを示し、各々の拡大Ｓ－ｂｏｘ内において、２０が後述する小ＭＤＳによる拡散部を示し、図中で最も小さく示した矩形（２１，２２）が入力側および出力側のＳ－ｂｏｘを示す。

【００３９】

図２において、Ｓ－ｂｏｘのうちハッチングしたものは活性を表し（図中の２１参照）、白抜きで示したものは差分零を表す（図中の２２参照）。また、太線で示した拡大Ｓ－ｂｏｘ（１１，１３，１６，１７，１９）は活性を表し、その他の拡大Ｓ－ｂｏｘ（１２，１４，１８）は差分零を表す。４段で活性Ｓ－ｂｏｘが２５個以上であることが分かる。

【００４０】

このように、本例の暗号では、２段で５×５＝２５個以上の活性Ｓ－ｂｏｘ数を保証できる。Ｓ－ｂｏｘの最大差分確率は、

$p_s = 6/256$、

２段での差分特性確率は、

$p_s^{25} = 2^{-135.4} << 2^{-128}$、

となり、差分解読法が有効でないことが分かる。

【００４１】

同様に、線形特性確率についても、

$q_s = 22/256$、

$q_s^{25} = 2^{-88.5} << 2^{-64}$、

となり、線形解読法が有効でないことが分かる。

【００４２】

なお、従来のＳＱＵＡＲＥ／Ｒｉｊｎｄａｅｌ型暗号に適用されるＳＱＵＡＲＥ攻撃は、段内の１バイトに対して、他の入力を固定したまま、2^8 通りのすべてのパターンを入力したとき、２段通過後の出力バイトの各々に対して2^8 通りのすべてのパターンが出現する特性を利用するものであるが、本例の暗号では、例えば後述する大ＭＤＳの取り方によってＳ－ｂｏｘ間の攪拌性を向上させることで、その単純な適用を困難にしている。

【００４３】

以下では、入れ子型暗号方式の具体例を用いながら本実施形態についてより詳しく説明する。

【００４４】

本実施形態の具体例の構成について説明する。

【００４５】

図３に、本実施形態の入れ子型暗号方式のデータ攪拌部の階層構造の例を示す。

【００４６】

ブロック長は、１２８ビットを例にとる（もちろん、他のブロック長でも本発明は実施可能である）。

鍵長は、２５６ビットを例にとる（もちろん、他の鍵長でも本発明は実施可能である）。なお、本実施形態で、ブロック長を１２８ビットとしたときに、鍵長を１２８ビットや１９２ビットとした場合について後述する。

【００４７】

複数並列された拡大Ｓ－ｂｏｘと大ＭＤＳとの対（ただし、後述するように最終段は大ＭＤＳを含まない）を１段と数えるものとした場合に、段数をＲ段として表し、具体例を用いる場合にはＲ＝８を用いる。なお、基本的には段数は何段でも実施可能であるが、実際の段数は、例えば安全性や計算機資源等を想定して適宜設定することができ、好ましくは６段以上、より好ましくは８段以上とすると、より効果的である。

【００４８】

なお、本例の暗号では、段関数がＳ－ｂｏｘ層を２層含んでいるので、１段が通常の２段に相当する。段構造内の大ＭＤＳについては、異なるガロア体に基づくいくつかの実装を示す（強度優先や速度優先の例を挙げる）。

【００４９】

図４に、本実施形態に係る暗号化装置の構成例を示す。

【００５０】

１０１が各段であり、１０４は大ＭＤＳ拡散層、１０２は拡大Ｓ－ｂｏｘ層、１０３は各々の拡大Ｓ－ｂｏｘである。１０５は、排他的論理和部である。１２１～１２４は、詳しくは後述する鍵スケジュール部の構成部分である。Ｐは入力となる１２８ビットの平文データ、Ｃは出力となる１２８ビットの暗号文データである。

【００５１】

段関数は、以下に述べるように、２段ＳＰＮ構造からなる３２ビット処理サブ・ブロック（拡大Ｓ－ｂｏｘ）１０３を４個並列に並べ、ＭＤＳ拡散層１０４で繋いだ構造である。全体の基本構造は、この段関数の繰り返しにする。

【００５２】

なお、図４の例では、暗号化と復号の処理を対称的にするため、最終段は拡大Ｓ－ｂｏｘ層１０２とその後の鍵加算１０５だけで構成することにしている。

【００５３】

段関数１段に２段ＳＰＮ構造が埋め込まれ、最後に鍵加算が行われるので、拡大鍵のビット長は、２×１２８×Ｒ＋１２８＝１２８（２Ｒ＋１）となる。Ｒ＝８の場合には、１２８×１７ビットとなる。

【００５４】

次に、Ｓ－ｂｏｘについて説明する。

【００５５】

本例の暗号では、入出力表で定義する８ビットＳ－ｂｏｘを利用する。

【００５６】

図５に、８ビットＳ－ｂｏｘの入出力表の一例を示す。図５において、配列要素は１６進数で表現してある。

【００５７】

図５の表は、最左上の値（７２）がｓ［０］に対応し、その１つ右の値（ＡＡ）がｓ［１］に対応し、その行の右端の値（９Ｆ）がｓ［１５］に対応し、次の行に移って、その左端の値（６９）がｓ［１６］に対応し、その１つ右の値（６Ａ）がｓ［１７］に対応し、以下同様の要領である。そして、最下右の値（５７）がｓ［２５５］に対応する。

【００５８】

図５に例示したＳ－ｂｏｘの特性は、次の通りである。

・最大差分確率：６／２５６（理論的最小値は４／２５６）

・最大線形確率：２２／２５６（理論的最小値は１６／２５６）

・代数次数：７次（全単射関数の最大値）

なお、Ｓ－ｂｏｘには、入出力表を用いる代わりに、演算処理を用いても良い。

【００５９】

次に、各々の拡大Ｓ－ｂｏｘ（または小構造とも呼ぶ）の部分について説明する。

【００６０】

図６に、拡大Ｓ－ｂｏｘ１０３の内部構成例を示す。この例では、４並列の８ビットＳ－ｂｏｘ１１２（図５参照）を２組用意し、拡散層１１３を挟んだ２段ＳＰＮ構造になっている。この構造は、ＳＰＳ構造と呼ぶべきものでもあるが、２段目の拡散層が省略された特殊な２段ＳＰＮ構造とみなす。Ｓ－ｂｏｘ１１２の入力直前では、必ず鍵加算１１１を行う。拡大Ｓ－ｂｏｘ内の拡散層１１３には、ＭＤＳ行列を使用し、これを小ＭＤＳと呼び、MDS_Sと表記する。小ＭＤＳのブランチ数は５である。

【００６１】

図７に、本例の暗号で利用するMDS_S行列の一例を示す。図７において、行列要素は１６進数で表現してある。ここで、Ｓ－ｂｏｘ入出力と行列要素は、乗算の際、ガロア体ＧＦ（2^8）の元とみなす。この例の場合の原始多項式は、$x^8+x^6+x^5+x+1$である。

【００６２】

次に、本例の暗号の段関数である大構造について説明する。

【００６３】

図８に、１段の部分の構成例を示す。本例の暗号の段関数である大構造は、４並列の３２ビット拡大Ｓ－ｂｏｘ１０３（図６参照）をＭＤＳ行列の拡散層１０４で結合して構成する。この段関数である大構造における拡散層１０４にも、ＭＤＳ行列を使用し、これを大ＭＤＳと呼び、MDS_Lと表記する。ただし、ここでのＭＤＳ行列とは、拡大Ｓ－ｂｏｘに着目したブランチ数が５であることを意味する。

【００６４】

大ＭＤＳの最も単純な構成は、拡大Ｓ－ｂｏｘの３２ビット幅の出力をＧＦ（

2^{32}）の元として実現する方法である。この方法は高い強度が実現しやすいが、一般的な実行は困難もしくは高速化はしにくい。そこで、この場合には、大ＭＤＳ行列に制約を課すのが好ましい。

【００６５】

また、４並列のＭＤＳを構成するには、４ビット幅で十分であり、ＧＦ（2^4）上の演算を利用して実現できる。さらに、ＭＤＳを巡回的なものにすることで、効率的な計算が可能になる。

【００６６】

また、実際には、これ以外のＧＦ（2^8）やＧＦ（2^{16}）を利用する中間の型も可能である。

【００６７】

ＧＦ（2^{32}）を利用した大ＭＤＳについて説明する。

【００６８】

この場合、拡大Ｓ－ｂｏｘの入出力をＧＦ（2^{32}）の元とみなして、大構造ＭＤＳを設計する。これは、ＳＰＮ構造での自然な設計法である。しかし、３２ビット幅では乗算表による実装は現実的ではない。計算による場合も一般のＭＤＳ行列では計算量が掛かり高速化が困難である。計算量が増加する原因は、ガロア体上の乗算における桁上がり時の処理が重いためである。計算量を抑えるためには、大ＭＤＳ行列を、ビット表現で３２ビット中の下位５ビットにのみ１が現れる（下位５ビット以外は０のものに限定した）要素で構成する方法がある。このような条件を満たす行列を使用することで、桁上がり処理を上位４ビットを入力とする表引きで処理可能となる。

【００６９】

図９に、大ＭＤＳ行列の一例を示す。この例の場合の原始多項式は、$x^{32}+x^{28}+x^{27}+x+1$である。

【００７０】

ＧＦ（2^4）を利用した大ＭＤＳについて説明する。

【００７１】

図１０に、この場合のＭＤＳ行列の一例を示す。この例の場合の原始多項式は

、x^4+x+1とする。

【００７２】

ここでは、１つの拡大Ｓ－ｂｏｘ１０３において４つのＳ－ｂｏｘの各々の出力すなわち８ビット・データの同じ位置（例えば図１０では最上位ビットを例にとって示している）の１ビットを集めて、これを１組４ビットのデータとし、４つの拡大Ｓ－ｂｏｘ１０３からの４組の４ビット・データを、ＧＦ（2^4）の元とみなす。

【００７３】

そして、８ビット・データの同じ位置について、２段の４並列拡大Ｓ－ｂｏｘ層の間の拡散層１０４に４行４列のＭＤＳ行列（例えば図１０では最上位ビットの場合、１０４－１）を用いる。

【００７４】

出力となった４組の４ビット・データは、それぞれ対応するもとの８ビット・データの同じ位置に結線される。

【００７５】

Ｓ－ｂｏｘのビット幅に対応して、８個のＭＤＳ行列（１０４－１～１０４－８）を用意して、大ＭＤＳとする。

【００７６】

これらの４行４列のＭＤＳ行列は、それぞれ、ブランチ数５を保証する。各ＭＤＳ行列は、Ｓ－ｂｏｘ中の異なるビット位置に接続するので、全体としてもブランチ数５を保証する。

【００７７】

各拡大Ｓ－ｂｏｘの同じ位置のＳ－ｂｏｘ出力を単位とした表引きによって（なお、演算によってもよい）、８個のＭＤＳ行列を同時に処理する効率的な実行が可能である。

【００７８】

さらに、ＭＤＳ行列が巡回的な場合、３２ビットごとの排他的論理和と８ビット単位のビット回転を組み合わせた効率的な処理が可能となる。

【００７９】

なお、上記と同様の考え方により、８ビット・データのうちの同じ位置の２ビットごとに処理を行うこととして、各要素が８ビットの４行４列のＭＤＳ行列（ＧＦ（2^8））を、４個用意して、大ＭＤＳとすることも可能である。また、８ビット・データのうちの同じ位置の４ビットごとに処理を行うこととして、各要素が１６ビットの４行４列のＭＤＳ行列（ＧＦ（2^{16}））を、２個用意して、大ＭＤＳとすることも可能である。

【００８０】

なお、図４では、拡大Ｓ－ｂｏｘを４並列で表しているが、これに限定されるものではなく、それ以外の並列数も可能である。

また、拡大Ｓ－ｂｏｘの内部構成を、全て同一とせずに、異なるものを混在させることも可能である。

また、全ての大ＭＤＳ行列を同一にせずに、異なるものを混在させることも可能である。この点は、小ＭＤＳ行列、Ｓ－ｂｏｘの入出力表についても同様である。

また、例えば、最初の入力段と、最後の出力段だけ、他の中間段とは異なる内部構成にしてもよい。

この他にも、種々のバリエーションが考えられる。

【００８１】

次に、鍵スケジュール部（鍵生成部）について説明する。

【００８２】

図１１に、鍵スケジュール部の構成例を示す。１２１は、データ攪拌部の段関数の１段分に対応する部分であり、１３１は線形拡散層（本例では、大ＭＤＳによる拡散層とする）であり、１３２は非線形変換層（本例では、４並列のＳＰ層（Ｓ－ｂｏｘ層・拡散層）１３３とする）であり、１３４は排他的論理和部であり、１３５は剰余加算部である。図１１では省略しているが、１２１の部分の構成が必要に応じて繰り返されることになる。なお、１２８ビットの鍵を出力する構成単位を鍵スケジュール部の１つの段とすると、鍵スケジュール部の段数は（２Ｒ＋１）段となる（Ｒ＝８の場合、１７段である）。

【００８３】

図１１の例では、２５６ビットの変形Ｆｅｉｓｔｅｌ型繰り返し処理の各段の出力左半分１２８ビットを取り出し、段数依存定数C_iを剰余加算して拡大鍵とする。

【００８４】

なお、鍵長を２５６ビットとする場合には、例えば、上位１２８ビットを初段の線形拡散層１３１に与え、下位１２８ビットを非線形変換層１３２に与えればよい。また、鍵長を１２８ビットとする場合には、例えば、その１２８ビットを初段の線形拡散層１３１に与えるとともに、非線形変換層１３２に与えればよい。また、鍵長を１９２ビットとする場合には、例えば、上位１２８ビットを初段の線形拡散層１３１に与え、下位側６４ビットと上位側６４ビットとを結合した１２８ビットを非線形変換層１３２に与えればよい。

【００８５】

なお、図１２のように、段数依存定数C_iを剰余加算する箇所について、種々のバリエーションが考えられる。

【００８６】

図１３に、図１１や図１２における非線形変換層１３２の各々の非線形変換層１３３の構成例を示す。１４１はＳ－ｂｏｘであり、１４２は４並列のＳ－ｂｏｘを入力とする小ＭＤＳである。

【００８７】

なお、このＳ－ｂｏｘは、図４の暗号処理側のＳ－ｂｏｘと同じものでもよいし、異なるものでもよい。小ＭＤＳについても同様である。また、鍵スケジュール部の各段によってＳ－ｂｏｘや小ＭＤＳの構成を変えることも可能である。

【００８８】

図１４に、図１１や図１２における非線形変換層１３２の各々の非線形変換層１３３の他の構成例を示す。この例は、図１３の構成に対して、排他的論理和部１４３を付加したものである。

【００８９】

さらに、図１４において、Ｓ－ｂｏｘに対する入力と排他的論理和をとる定数を、段数依存定数とする構成も可能である。

【００９０】

次に、各段で異なる定数C_iを作る方法の一例について説明する。

【００９１】

図１１や図１２の鍵スケジュール部の１２８ビットの加算定数C_iは、４つのビット定数（H_0，H_1，H_2，H_3）の組み合わせで記述することができる。３２ビットの定数H_iの一例を次に示す。

H_0＝（５ａ８２７９９９）$_H$＝$2^{1/2}$／４

H_1＝（６ｅｄ９ｅｂａ１）$_H$＝$3^{1/2}$／４

H_2＝（８ｆ１ｂｂｃｄｃ）$_H$＝$5^{1/2}$／４

H_3＝（ｃａ６２ｃ１ｄ６）$_H$＝$10^{1/2}$／４

加算定数C_iの組み合わせを、C_i＝（C_{i0}，C_{i1}，C_{i2}，C_{i3}）と記述する。各段で異なる１２８ビットの定数C_iを容易に生成するため、C_iを構成するH_iの組み合わせの決定に８ビットＬＦＳＲを用いる。例えば、ＬＦＳＲの原始多項式には（１Ｄ）$_H$を、ＬＦＳＲの初期状態には（８Ｂ）$_H$を用いる。このＬＦＳＲを用いて生成されたビット列を２ビットづつ読み出し、定数として使用する３２ビット定数H_iを決定する。

【００９２】

図１５に、上記のような方法によりＬＦＳＲを用いて決定した加算定数表の例を示す。

【００９３】

なお、ＬＦＳＲの初期状態は、可変としてもよいし、固定としてもよい。前者の場合には、ＬＦＳＲの初期状態も鍵の一部を構成することになる。後者の場合には、暗号側と同じＬＦＳＲの初期状態を持つ復号側のみ、暗号文を復号することができる。

【００９４】

以上説明したような鍵スケジュール部によれば、非線形変換層については、入力の１ビットが変化すると、Ｓ－ｂｏｘ（１４１）により、８ビットに変化を波及させ、さらに、小ＭＤＳ（１４２）により、３２ビットに変化を波及させることができる。さらにまた、線形拡散層については、大ＭＤＳ（１３１）が前段の

非線形変換層の出力をより大きく攪拌するので、１ビットの違いも、１２８ビットの幅に広がる利点がある。

【００９５】

従って、このような鍵スケジュール部によれば、各段でバラバラな鍵が出やすい、攪拌しやすい、という効果を得ることができる。また、段ごとに異なる定数により、段にわたる鍵の一致が少ない（鍵がほぼ一致しない）、という効果を得ることができる。

【００９６】

さて、以下では、大きなブロック長を持つブロック暗号のデータの攪拌部に用いられる効率的な線形拡散装置について説明する。

【００９７】

図１６に、本実施形態の線形拡散装置の基本的な構成要素である有限体乗算装置の構成例を示す。前述したＧＦ（2^{32}）あるいはＧＦ（2^{16}）を利用した大ＭＤＳ（図９、図４の１０４、図１１や図１２の１３１参照）における、１つの入力と大ＭＤＳ行列の１つの要素との積の計算に、この線形拡散装置を用いることができる。

【００９８】

図１６に示されるように、この有限体乗算装置は、係数格納部２０２、乗算部２０３、桁溢れ帰還部２０１、排他的論理和部（排他和部）２０４を用いて構成される。

【００９９】

係数格納部２０２は、係数すなわち乗算の乗数（例えば、図９の大ＭＤＳ行列の１つの要素）を格納する部分である。

【０１００】

乗算部２０３は、入力ワードと係数を２進数とみなした場合の乗算を行う部分である。

【０１０１】

桁溢れ帰還部２０１は、乗算の結果として生ずる桁溢れを有限体上の乗算に戻すため排他的論理和部２０４で足される数（帰還ワード）を検索する部分である

。

【０１０２】

排他的論理和部２０４は、乗算部２０３の出力と桁溢れ帰還部２０１の出力ビット的な排他和を行う部分である。

【０１０３】

有限体乗算装置２００の機能は、有限体ＧＦ（２）の拡大体ＧＦ（2^k）の元である入力ワードａと同じ有限体の別の元である係数ｂの積ａ×ｂを出力ワードとして計算することである。

【０１０４】

まず、有限体における積について説明する。

【０１０５】

なお、以下の記述において、$\Sigma a_i x^i$ において総和を取るｉの範囲や$\Sigma b_j x^j$ において総和を取るｊの範囲を０～ｋ－１とし、それらの範囲についての記述を省略する。

【０１０６】

ＧＦ（2^k）の元は、多項式表現によって、ある変数ｘの（ｋ－１）次の多項式$\Sigma a_i x^i$ として表現できる。元ａを表現するのに、その係数を並べて$c_{k-1} c_{k-2} \cdots c_0$ として表現することもある。

【０１０７】

２つの元$a=\Sigma a_i x^i$ と$b=\Sigma b_i x^i$ の積は、

$$a \times b = (\Sigma a_i x^i) \times (\Sigma b_i x^i) \mod p(x)$$

で定義される。

【０１０８】

ここで、ｐ（ｘ）はＧＦ（2^k）の原始多項式と呼ばれ、周期（2^k-1）を持つｋ次の既約なモニック多項式である。また、ｍｏｄの意味は、例えば、ｋ＝３２の場合、原始多項式としてｐ（ｘ）＝$x^{32}+x^{28}+x^{27}+x+1$を選んだ場合、多項式の積によってx^{32}の項や因子が現れた場合には、それを（$x^{28}+x^{27}+x+1$）と見なすということを表す。従って、積もまたｋ次未満の多項式となる。

【０１０９】

一般に、このような操作を行う場合、高速な処理を行うため、乗数と被乗数をタグとして積を検索する乗算表を用いた乗算装置を用いることがある。しかし、乗数と被乗数はともに2^k個の値を取り得るので、乗算表は、2^{2k}個のエントリを持ち、各エントリはｋビットのサイズを持つので、ｋがある程度大きくなると、乗算表のサイズは非常に大きなものとなる。

【０１１０】

本実施形態も、基本的には、乗算表を用いる方式に類似するが、係数がある制約条件を満足する場合には、はるかに小さな記憶容量によって実現することができる。

【０１１１】

その制約条件とは、係数ｂは、定数であって、非零の係数を持つのは、ある次数ｔ以下の下位の係数のみであるということである（ｔ次を越える次数の係数は０であり、ｔ次以下の係数は０または１である）。ある元ａが任意の元を取る場合には、桁溢れは、最大３２ビットであるが、この制約条件を満足する場合には、桁溢れは、高々、ｔビットである。このｔビットの桁溢れの値を決定するのは、被乗数ａの上位ｔビットまでのＭＳＢ（Ｍｏｓｔ　Ｓｉｇｎｉｆｉｃａｎｔ　Ｂｉｔｓ）である。

【０１１２】

有限体上の乗算と通常の多項式と見なした場合の乗算との違いは、２進数の積の結果、３２次以上の係数への桁溢れが起こった場合に、原始多項式によって、３２次未満の係数へその寄与を還元する必要があるが、本実施形態では、桁溢れ帰還部２０１が、還元すべきワードを表として持っている。

【０１１３】

この帰還ワードは、高々（ｔ＋１）ビットの係数ｂと乗数ａの上位ｔビットと原始多項式から決定できる。つまり、（ａ［（ｋ－ｔ）...（ｋ－１）］×ｂ）［（ｔ＋１）...２ｔ］　ｍｏｄ　ｐ（ｘ）によって与えられる。ここで、ａ［（ｋ－ｔ）...（ｋ－１）］とは、ａの中から、（ｋ－１）次から（ｋ－ｔ）次までの項を取り出したものである。

【０１１４】

すなわち、桁溢れ帰還部２０１が持つ帰還ワードの表の内容は、対応するＭＤＳ行列（図９参照）の要素に応じて決まる。

【０１１５】

桁溢れ帰還部２０１が持つ帰還ワードの表は、2^t 個のエントリからなり、各エントリはｋビットのサイズを持つ。

【０１１６】

次に、上述した有限体乗算装置を利用することで実現される、ブロック暗号のデータ・ブロックに線形変換を施す線形変換装置について説明する。

【０１１７】

線形変換の１種にＭＤＳ行列による線形変換がある。ＭＤＳ行列とは、データ・ブロックが、複数（ｎ）のワードから構成され、各ワードがｋビットの長さを持つ場合、各ワードを有限体ＧＦ（2^k）の元と見なし、ｎ個の元の組をｎ個の元の組に線形写像するｎ行ｎ列の行列であって、すべての小行列が非零のものである。ＭＤＳ行列による線形変換は、非零の入出力のワードの数の下限が保証されているという性質を持つ。

【０１１８】

しかし、一般に、有限体ＧＦ（2^k）上の行列演算は、ＧＦ（2^k）上の複数回の乗算と加算から構成され、計算コストが大きい。

【０１１９】

図１７に、本実施形態の線形変換装置の構成例を示す。前述したＧＦ（2^{32}）あるいはＧＦ（2^{16}）を利用した大ＭＤＳ（図９、図４の１０４、図１１や図１２の１３１）に、この線形変換装置を用いることができる。

【０１２０】

図１７の構成では、まず、図１６の有限体乗算装置をＭＤＳ行列に対応してマトリクス状に用意する。

【０１２１】

図１７においてｍ＝ｎとすると、n^2 個の有限体乗算装置２００の各々の係数は、ｎ行ｎ列のＭＤＳ行列の対応する要素と同じ値をとる。係数 a_{ij} を持つ装置

には、第ｉ入力ワードが入力される。

【０１２２】

各々の出力ワードに対する排他的論理和部（排他和部）２０５は、それぞれ、あるｊに対応する係数a_{ij}を持つすべての有限体乗算装置２００の出力ビット的な排他的論理和を計算し、第ｊ出力ワードとして出力する。

【０１２３】

本実施形態における線形変換装置は、線形変換を表現するＭＤＳ行列を（a_{ij}）で表現するとき、各要素a_{ij}は高々ｔ次までの項しか非零の係数を持たないことを特徴とする。ここで、ｉ，ｊは、０からｎ－１までの整数値を取りうるとする。また、ｔは、有限体ＧＦ（2^k）の拡大次数ｋよりも小さな正数であるとする。

【０１２４】

これによって、図１８のような乗算が実現できる。

【０１２５】

なお、桁溢れ帰還部２０１が持つ帰還ワードの表の内容は、対応するＭＤＳ行列の要素に応じて決まるので、例えば、図９の大ＭＤＳ行列の例では、４種類の帰還ワード表だけ持てばよいことになる。

【０１２６】

次に、本暗号方式に用いるＭＤＳ行列（特に大ＭＤＳ）を生成するためのＭＤＳ行列生成装置（もしくはランダム生成アルゴリズム）について説明する。

【０１２７】

図１９に、ＭＤＳ行列生成装置の構成例を示す。図１９に示されるように、このＭＤＳ行列生成装置は、要素生成部２３１、小行列式計算部２３２、判定部２３３を用いて構成される。

【０１２８】

図２０に、この場合の手順の一例を示す。

【０１２９】

要素生成部２３１は、ランダムに、ｎ行ｎ列のＭＤＳ行列の各行列要素を生成する（ステップＳ１）。なお、先の有限体乗算装置を適用可能とする場合には、

このときに、下位ｔビットのみ非零の要素（ｔ次以下の要素）からなるＭＤＳ行列を生成しておく（すなわち、この場合には、要素生成部２３１内で、下位ｔビットのみ非零かどうかのチェックを行うことになる）。

【０１３０】

なお、行列要素を生成するためには、乱数を発生して用いる方法や、多重ループの制御変数の値を用いる方法など種々の方法が考えられる。

【０１３１】

次に、小行列式計算部２３２は、要素生成部２３１の生成した行列の１次小行列を計算し（ステップＳ２）、判定部２３３は、小行列式計算部２３２が計算した小行列が非零か否かを判定する（ステップＳ３）。１つでも零の１次小行列式があれば、ステップＳ１からやり直す。

【０１３２】

すべての１次小行列式が非零ならば、同じ要領で、２次小行列について同様にチェックする（ステップＳ４，Ｓ５）。

【０１３３】

以上を、ｎ次小行列式まで、同じ要領で行い（ステップＳ６，Ｓ７）、１次からｎ次まですべての小行列式が非零であることが確認されたならば、そのＭＤＳ行列を出力する（ステップＳ８）。

【０１３４】

なお、ステップＳ８で得たＭＤＳ行列を暗号化に用いるＭＤＳ行列とした場合、復号に用いるＭＤＳ行列は、ステップＳ８で得たＭＤＳ行列の逆行列によって与えられる（逆に、ステップＳ８で得たＭＤＳ行列を復号に用いる場合には、その逆行列が、暗号化に用いるＭＤＳ行列となる）。

【０１３５】

ただし、ステップＳ８で得られたＭＤＳ行列の全ての要素が下位ｔビットのみ非零であっても、その逆行列の全ての要素が下位ｔビットのみ非零であるとは限らない。

【０１３６】

なお、図２０の手順おいて、小行列式の判定を１次からｎ次まで順番に行って

いるが、他の順番でもよく、また、それらの全部または一部を並列して行ってもよい。

【０１３７】

次に、暗号化に用いるＭＤＳ行列と、その逆行列である、復号に用いるＭＤＳ行列との両方とも、下位ｔビットのみ非零という条件を満たすように、ＭＤＳ行列を求める方法について説明する。

【０１３８】

図２１に、この場合のＭＤＳ行列生成装置の構成例を示す。図２１に示されるように、このＭＤＳ行列生成装置は、要素生成部２３１、小行列式計算部２３２、判定部２３３、逆行列生成部２３４、逆行列判定部２３５を用いて構成される。要素生成部２３１、小行列式計算部２３２、判定部２３３の部分は、図１９と同様である。

【０１３９】

図２２に、この場合の手順の一例を示す。

【０１４０】

まず、先の例と同様にして、要素生成部２３１、小行列式計算部２３２、判定部２３３により、下位ｔビットのみ非零の要素からなるＭＤＳ行列を生成する（ステップＳ１１）。

【０１４１】

次に、逆行列生成部２３４により、生成されたＭＤＳ行列の逆行列を求める（ステップＳ１２）。

【０１４２】

次に、逆行列判定部２３５は、求められた逆行列の各々の要素が、下位ｔビットのみ非零かどうか調べる。

【０１４３】

全ての要素が下位ｔビットのみ非零であれば（ステップＳ１３）、そのＭＤＳ行列および逆行列を出力する（ステップＳ１４）。

【０１４４】

1つでも下位ｔビットのみ非零ではない要素があれば（ステップＳ１３）、Ｓ

１１からやり直す。

【０１４５】

なお、ステップＳ１１で生成されたＭＤＳ行列を暗号化に用いる場合、ステップＳ１２で生成された逆行列を復号に用いることになる（逆に、ステップＳ１１で生成されたＭＤＳ行列を復号に用いる場合、ステップＳ１２で生成された逆行列を暗号化に用いることになる）。

【０１４６】

なお、ＭＤＳ行列を生成するにあたっては、同一行内に同じ値の要素が存在しないようなＭＤＳ行列（ｎ行ｎ列のＭＤＳ行列において第ｉ１要素から第ｉｎ要素までの中に同一の値を持つ２個以上の要素がないもの）を生成するようにしてもよい。例えば、図２０や図２２の手順例の場合、ＭＤＳ行列の生成時に、同一行内に同じ値の要素が存在するかどうかチェックし、同一行内に１つでも同じ値の要素が存在すれば、ＭＤＳ行列を生成し直すようにすればよい。なお、同一列内に同じ値の要素が存在しても構わない。

【０１４７】

ブロック暗号のデータの線形変換装置として、同一行内に同じ値の要素が存在しないようなＭＤＳ行列を選択した線形変換装置を用いることによって、入力ワードの差分値が相殺する確率を小さくすることができる。

【０１４８】

また、同一行内の要素の和が１または０にならないようにＭＤＳ行列を生成するようにしてもよい。この場合も、同様の効果が得られる。

【０１４９】

次に、Ｓ－ｂｏｘと小ＭＤＳの組み合わせを選択する（あるいは最適化する）ことによって、より安全性を高める方法、より具体的には、最大差分特性確率が理論的最悪例よりも良くなることを保証するＳ－ｂｏｘとＭＤＳの組み合わせの設計方法について説明する。

【０１５０】

ＭＤＳはブランチ数Ｂしか保証しないので、Ｓ－ｂｏｘの最大差分確率がｐとすると、最大差分特性確率は、p^B になる。例えば、ｍ行ｍ列のＭＤＳはＢ＝ｍ

＋１となる。しかし、Ｓ－ｂｏｘと小ＭＤＳの組み合わせを選択する（あるいは最適化する）ことにより、ブランチ数Ｂで、最大差分特性確率がp^B未満を保証することができる。この結果、通常のＭＤＳよりも最大差分確率が小さいＭＤＳとＳ－ｂｏｘを組み合わせることにより、相乗効果が望め、安全性をより向上させることができる。

【０１５１】

さて、暗号アルゴリズムの安全性評価の一手法として、差分解読法あるいは線形解読法があり、両者は双対な関係にある。差分解読法に着目すると、Ｓ－ｂｏｘの安全性は入出力の差分相関を持つ確率で規定され、この確率が小さいほど安全性が高い。暗号アルゴリズムでは、差分確率の小さいＳ－ｂｏｘが多数組み合わせられるほど安全性が向上する。効率的なＳ－ｂｏｘの連結方法として、線形変換装置が従来から提案されている。線形変換装置は、あるブロック長のデータに対して線形変換を施す装置で、暗号化装置（や復号装置）の構成要素として利用されることがある。線形変換の一種にＭＤＳ行列による線形変換がある。

【０１５２】

ＭＤＳ行列とは、データブロックがｎ個の複数のワードから構成される場合、ｎ個のワードへの線形変換を定義する行列であり、非零の入出力ワードはｎ＋１個以上が保証されているという性質を持つ。しかし、Ｓ－ｂｏｘは、差分確率として、６／２５６、４／２５６、２／２５６など複数の値の候補を持つため、ＭＤＳであっても、ｎ＋１個の確率がそれぞれ６／２５６のＭＤＳと、それぞれ４／２５６であるＭＤＳとでは、後者の方が安全性が高い。

【０１５３】

従来、Ｓ－ｂｏｘとＭＤＳは単体の構成要素としてそれぞれ独立に安全性を評価されたが、ここでは、Ｓ－ｂｏｘとＭＤＳの相乗効果を検証する装置の例を示す。

【０１５４】

図２３に、この場合の処理手順の一例を示す。この例は、差分解読法に着目して、Ｓ－ｂｏｘとの相乗効果が望めるＭＤＳ決定処理を示している。差分解読法と線形解読法は双対な関係にあるため、この処理を線形確率に着目して行うこと

により、線形解読法に対しても同じ効果が得られる。

【０１５５】

まず、複数のＳ－ｂｏｘの候補と複数の小ＭＤＳの候補を生成する（ステップＳ２１、ステップＳ２２）。なお、ステップＳ２１とステップＳ２２は逆の順番で行ってもよいし、並列して行ってもよい。

【０１５６】

次に、Ｓ－ｂｏｘ候補のなかからＳ－ｂｏｘを１つ選択するとともに（ステップＳ２３）、小ＭＤＳ候補のなかから小ＭＤＳを１つ選択する（ステップＳ２４）。なお、ステップＳ２３とステップＳ２４を逆の順番で行ってもよいし、並列して行ってもよい。

【０１５７】

次に、後述するように、有効な（活性にした）Ｓ－ｂｏｘの差分値の最大を計算し（ステップＳ２５）、上限（例えば、６／２５６）を下回る差分値（例えば、４／２５６）が含まれているかどうか調べる。

【０１５８】

そして、含まれていれば（ステップＳ２６）、そのときのＳ－ｂｏｘと小ＭＤＳの組み合わせを出力する（ステップＳ２７）。

【０１５９】

一方、含まれていなければ（ステップＳ２６）、Ｓ－ｂｏｘと小ＭＤＳの一方または両方を選択し直して、以下、同様に、処理を繰り返す。

【０１６０】

なお、図２３では、最初に複数のＳ－ｂｏｘの候補と複数の小ＭＤＳの候補を生成しておいたが、その代わりに、最初の１組以外は、ステップＳ２６で条件を満たさずに、他のＳ－ｂｏｘおよびまたはＭＤＳを選択することになったときに、生成するようにしてもよい。

【０１６１】

ステップＳ２５およびステップＳ２６の処理は、実際には、次のようになる。

【０１６２】

例えば、図６の例の場合、Ｓ－ｂｏｘと小ＭＤＳの組について、次の４種類、

計２０通りの検証を行い、すべての条件を満たした場合に、ステップＳ２７でそのときのＳ－ｂｏｘと小ＭＤＳの組が出力される。

①小ＭＤＳ１１３の入力側の１つのＳ－ｂｏｘ１１２のみ活性にした場合に、小ＭＤＳ１１３の出力側の４つのＳ－ｂｏｘ１１２が全て活性になり、かつ、そのうちの１つでも上限を下回る差分値になれば、この検証を合格とする。この検証を、入力側の４つのＳ－ｂｏｘ１１２の各々について行う（４通りある）。

②小ＭＤＳ１１３の入力側の２つのＳ－ｂｏｘ１１２のみ活性にした場合に、小ＭＤＳ１１３の出力側の４つのＳ－ｂｏｘ１１２が全て活性になれば、この検証を合格とし、小ＭＤＳ１１３の出力側の３つのＳ－ｂｏｘ１１２が活性になり、かつ、そのうちの１つでも上限を下回る差分値になれば、この検証を合格とする。この検証を、入力側の２つのＳ－ｂｏｘ１１２の組み合わせの各々について行う（６通りある）。

③小ＭＤＳ１１３の出力側の２つのＳ－ｂｏｘ１１２のみ活性にした場合に、小ＭＤＳ１１３の入力側の４つのＳ－ｂｏｘ１１２が全て活性になれば、この検証を合格とし、小ＭＤＳ１１３の入力側の３つのＳ－ｂｏｘ１１２が活性になり、かつ、そのうちの１つでも上限を下回る差分値になれば、この検証を合格とする。この検証を、出力側の２つのＳ－ｂｏｘ１１２の組み合わせの各々について行う（６通りある）。

④小ＭＤＳ１１３の出力側の１つのＳ－ｂｏｘ１１２のみ活性にした場合に、小ＭＤＳ１１３の入力側の４つのＳ－ｂｏｘ１１２が全て活性になり、かつ、そのうちの１つでも上限を下回る差分値になれば、この検証を合格とする。この検証を、出力側の４つのＳ－ｂｏｘ１１２の各々について行う（４通りある）。

【０１６３】

上記の複数の検証処理は、逐次行ってもよいし、全部または一部を並列的に行ってもよい。上記の複数の検証処理のうち、１つでも合格しないものがあれば、そのＳ－ｂｏｘと小ＭＤＳの組み合わせについては、以降の全ての検証処理をうち切って、不合格として構わない。

【０１６４】

なお、図２３の手順の例では、最初に条件を満たしたＳ－ｂｏｘと小ＭＤＳの

組み合わせが得られた時点で、処理をうち切るものであったが、条件を満たしたＳ－ｂｏｘと小ＭＤＳの組み合わせを複数求め、それらのうちで最も良いと評価されるものを選択するようにしてもよい。

【０１６５】

以下では、復号側について説明する。

【０１６６】

復号側は、基本的には、暗号側を逆にした構造である（鍵は同一である）。

【０１６７】

図２４に、図４の暗号化装置に対応する復号装置の構成例を示す。

【０１６８】

図２５に、図６の小構造に対応する構成例を示す。

【０１６９】

図２６に、図８の大構造に対応する構成例を示す。

【０１７０】

なお、図２４では、復号装置の鍵スケジュール部は、図４の暗号化装置の鍵スケジュール部と同一の構成としてある。

【０１７１】

復号装置における、Ｓ－ｂｏｘ１１１２の入出力表、小ＭＤＳ１１１３の小ＭＤＳ行列、大ＭＤＳ１１０４の大ＭＤＳ行列は、それぞれ、暗号化装置における、Ｓ－ｂｏｘ１１２の入出力表（例えば図５）、小ＭＤＳ１１３の小ＭＤＳ行列（例えば図７）、大ＭＤＳ１０４の大ＭＤＳ行列（例えば、図９、図１０）と逆関数（逆行列）の関係になっている。

【０１７２】

なお、図２４では、鍵については、図４と同様の順番で生成しているが、図４とは逆の順番で生成するように構成することも可能である。

【０１７３】

図２７に、この場合の鍵スケジュール部の構成例を示す。

【０１７４】

１１３２は、図１１の非線形変換層１３２の逆変換を示している（例えば各々

のＳＰ層１３３の逆変換（例えば図１３あるいは図１４の入出力を逆方向にしたもの）を４並列にしたものである）。

【０１７５】

図２７の鍵スケジュール部で用いる、Ｓ－ｂｏｘの入出力表、小ＭＤＳ行列、大ＭＤＳ行列は、それぞれ、図１１の鍵スケジュール部で用いる、Ｓ－ｂｏｘの入出力表、小ＭＤＳ行列、大ＭＤＳ行列と逆関数（逆行列）の関係になっている。

【０１７６】

また、図２７の復号の鍵入力Ｋ’は、図４において（暗号側で）最後の鍵加算に用いられた鍵とする。

【０１７７】

なお、この場合においても、段数依存定数C_iを剰余加算する箇所について、図１２の場合と同様の方法をはじめとして、種々のバリエーションが考えられる。

【０１７８】

以下では、大ＭＤＳの好ましい一形態について説明する。

【０１７９】

入れ子型（再帰的）ＳＰＮ型暗号のＳＱＵＡＲＥ攻撃に対する安全性がＳＱＵＡＲＥ暗号／Ｒｉｊｎｄａｅｌ暗号より改善する一つの理由として、Ｓ－ｂｏｘ間（前段の拡大Ｓ－ｂｏｘの後半（あるいは最終段）のＳ－ｂｏｘと後段の拡大Ｓ－ｂｏｘの前半（あるいは初段）のＳ－ｂｏｘとの間）に設けた大ＭＤＳ拡散層による攪拌性があげられるが、ここでは、ＳＱＵＡＲＥ攻撃に対する耐性をより効果的なものにするための大ＭＤＳの構成についての選択基準の例を示す。

【０１８０】

ところで、通常、ＳＰＮ型暗号に対するＳＱＵＡＲＥ攻撃では、

①可変ｂｙｔｅは全２５６パターンを取る、

②他のｂｙｔｅは固定、

という条件を満たす２５６パターン（Λ集合）を入力し、そして、２５６パターンに対するビット和が０になる鍵を探索することによって、鍵を推定する、とい

う手順が取られる。

【０１８１】

これを背景として、大ＭＤＳの結合（大ＭＤＳの入力側と出力側のビット間の結合関係あるいは演算経路の配線関係）に一定の条件を加えることによって、ＳＱＵＡＲＥ攻撃に対する安全性を向上させる。この一定の条件とは、概略的には、差分経路（前段の拡大Ｓ－ｂｏｘの前半のＳ－ｂｏｘと後段の拡大Ｓ－ｂｏｘの前半のＳ－ｂｏｘとの間の演算経路）の全部または一部を複線化させる（ファン・イン（ｆａｎ－ｉｎ）を２以上にする）というものである。これによって、高いなだれ効果が得られ、従来に比較してＳＱＵＡＲＥ攻撃可能な段数を１段減らせることにができる。

【０１８２】

まず、図２８～図３５（各図においてデータは上側から下側へ流れるものとしている）を参照しながら、大ＭＤＳの一構成例を示す。この例は、全ての差分経路についてファン・インを２以上にするように、大ＭＤＳを構成した例である。

【０１８３】

なお、ここで説明する大ＭＤＳも、ハードウェア（例えば半導体基板上等に形成した実回路）によっても、機能的に等価な行列演算または入出力変換表による変換を実行するためのソフトウェアによっても実現可能であるが、図２８～図３５ではハードウェアによって実現する場合を想定して説明する。

【０１８４】

図２８に、図４の暗号システムや図２４の復号システムにおける大ＭＤＳ層（暗号側の場合は１０４－１～１０４－８で、復号側の場合は１１０４－１～１１０４－８）と、その前段および後段の４並列の拡大Ｓ－ｂｏｘ（暗号側の場合は１０３で、復号側の場合は１１０３）、そして拡大Ｓ－ｂｏｘを構成する４並列のＳ－ｂｏｘおよび小ＭＤＳを示す。ただし、図６等に示したような鍵加算は図２８以降の各図ではその記述を省略している。

【０１８５】

さて、図２８の例は、図１０と同様に、各Ｓ－ｂｏｘの８ビットのうちの１ビットを抜き出したものについてそれぞれ独立に同一処理を行う構成を取っている

。図２８は、各Ｓ－ｂｏｘの８ビットのうちの最も左側の１ビットを抜き出したもの（１６ビットデータあるいは４組の４ビットデータ）について処理を行うＭＤＳ部分１０４－１について説明している。なお、図２９では、各Ｓ－ｂｏｘの８ビットのうちの最も右側の１ビットを抜き出したものについて処理を行うＭＤＳ部分１０４－８について説明している。また、図示はしていないが他の６ビットの各々についても同様である。

【０１８６】

図２８以降の各図で示す配線やレイアウトは論理的な関係を示すものであり、実配線や実レイアウトにはもちろん設計の自由度がある。また、図２８の例では、大ＭＤＳ層の各部分１０４－１～１０４－８の８つを実装するものとしているが、ＭＤＳ部分１０４－１～１０４－８のうちの一部（例えば、１つ、２つ、あるいは４つ）のみを実装し、それを時分割的に共用するように構成することも可能である。

【０１８７】

なお、暗号側と復号側で構成の仕方は同様であるので（逆変換の関係になるだけである）、以下では、暗号側を例にとって説明する。また、大ＭＤＳ層の各部分１０４－１～１０４－８は同一構成として、そのうちの１つの部分（１０４－１とする）について説明する。

【０１８８】

図３０に、大ＭＤＳ層の一つの部分（以下、単に大ＭＤＳと呼ぶ）１０４－１の前段の第１の拡大Ｓ－ｂｏｘ１０３－１－１の後半の４つのＳ－ｂｏｘと、大ＭＤＳの後段の４つの拡大Ｓ－ｂｏｘ１０３－２－１～１０３－２－４の前半における合計１６のＳ－ｂｏｘとの間の結合関係の一例を示す。なお、図３０～図３４において、ビットの配線が合流するところでは、排他的論理和によってそれら複数ビットが結合される（各図では、排他的論理和回路の記述を省略している）。

図３１に、大ＭＤＳの前段の第２の拡大Ｓ－ｂｏｘ１０３－１－２について、図３０と同様の関係を示す。

図３２に、大ＭＤＳの前段の第３の拡大Ｓ－ｂｏｘ１０３－１－３について、

図３０と同様の関係を示す。

図３３に、大ＭＤＳの前段の第４の拡大Ｓ－ｂｏｘ１０３－１－４について、図３０と同様の関係を示す。

図３０～図３３を参照すると、大ＭＤＳの後段の拡大Ｓ－ｂｏｘの同一のＳ－ｂｏｘには、いずれについても、それぞれ図３０～図３３のようにして排他的論理和により結合された４つのビットが結合されるが、それら４つのビットについても排他的論理和によって接合される。この様子を、大ＭＤＳの後段の第１の拡大Ｓ－ｂｏｘ１０３－２－１について、図３４に示す。大ＭＤＳの後段の他の拡大Ｓ－ｂｏｘ１０３－２－２～１０３－２－４については図示を省略するが、同様の結合関係である。なお、ここでは図３０～図３３のような排他的論理和による結合の後に図３４のような排他的論理和による結合を行ったように示しているが、それらすべての排他的論理和による結合を一括して行ってもよいし、適宜複数に分けて行ってもよい。

【０１８９】

さて、以上に例示した構成は、次の基準に基づいている。

【０１９０】

図４のような暗号回路において連続する２段（すなわち図３０～図３４）を考える。前段の拡大Ｓ－ｂｏｘ１０３における前半のＳ－ｂｏｘと、後段の拡大Ｓ－ｂｏｘ１０３の前半のＳ－ｂｏｘとは、前段の拡大Ｓ－ｂｏｘ１０３における後半のＳ－ｂｏｘを経由して接続されている。このときに、次の基準を大ＭＤＳ（１３０－１～１０３－８）の選択基準とする。

（１）前段の拡大Ｓ－ｂｏｘ１０３の前半における全Ｓ－ｂｏｘ（ここでは合計１６個のＳ－ｂｏｘ）のうちから任意に選んだ１つのＳ－ｂｏｘと、後段の拡大Ｓ－ｂｏｘ１０３の前半における全Ｓ－ｂｏｘ（ここでは合計１６個のＳ－ｂｏｘ）のうちから任意に選んだ１つのＳ－ｂｏｘとが、いずれもの組み合わせについても、２本以上の経路によって相互に接続（結合）されている。

（２）当該大ＭＤＳによってなされる線形拡散の逆変換もしくは逆関数（すなわち復号回路側の大ＭＤＳ）が存在し、かつ、それについても（１）と同じ条件が満たされる。

（１）については、例えば、図３５に示すように、１００１のＳ－ｂｏｘと１００２のＳ－ｂｏｘとが、矢印で示すような２本の経路によって相互に接続されており、他のＳ－ｂｏｘ間についても同様に２～４本の経路によって相互に接続されている。なお、これに対して、従来のＳＱＵＡＲＥ暗号／Ｒｉｊｎｄａｅｌ暗号では、図３６に示すように、１００３のＳ－ｂｏｘと１００４のＳ－ｂｏｘとの間は矢印で示すように１本のみの経路であり（ファン・イン＝１）、他のＳ－ｂｏｘ間についても同様である（したがって、なだれ効果は低い）。

（２）については、後述するように満たされている。

【０１９１】

ここで、上記基準を満たす構成におけるＳＱＵＡＲＥ攻撃に対する安全性について説明する。

【０１９２】

まず、ＳＱＵＡＲＥ攻撃で入力として用いるΛ（ラムダ）集合の定義を示す。

各データがｎ個のバイト（ｎは複数とする；なお１バイト＝８ビットである）を連結したものからなり、そのようなデータを２５６個含む集合があり、その２５６個の全データにおける各々のバイトの値について、次のいずれか一方が成立するとき、

（ａ）取り得る２５６（＝２＾８）種類の値が全部現れる

（ｂ）取り得る２５６（＝２＾８）種類の値のうちの１つのみが現れる（すなわち、常に値が固定）

この２５６個のｎバイトのデータの集合をΛ集合と呼ぶ。

Λ集合には、次の性質がある。

・Λ集合を入力とする並列Ｓ－ｂｏｘ（可逆）の出力の集合もまた、Λ集合である。

【０１９３】

値が固定でないバイトが１個だけあるΛ集合を、図３０～図３３のような上記基準を満たす構成における前段の拡大Ｓ－ｂｏｘ１０３の後半のＳ－ｂｏｘ群に入力としたとき、次の性質が確率１で成立する（図３５参照）。

（ｉ）Λ集合となるのは、前段の拡大Ｓ－ｂｏｘの後半のＳ－ｂｏｘの出力までである。

（ii）任意ビットの２５６パターンについての和が０になるのは、後段の拡大Ｓ－ｂｏｘの前半のＳ－ｂｏｘの入力位置までである。

【０１９４】

これに対して、従来のＳＱＵＡＲＥ暗号／Ｒｉｊｎｄａｅｌ暗号では、次の性質が確率１で成立する（図３６参照）。

（ｉ’）後段の前半のＳ－ｂｏｘ通過後もΛ集合である。

（ii’）後段の後半のＳ－ｂｏｘの入力位置の任意のビットを２５６パターンについて足すと０になる。

【０１９５】

このように、上記基準を満たす大ＭＤＳでは、従来のＳＱＵＡＲＥ暗号／Ｒｉｊｎｄａｅｌ暗号に比較してＳ－ｂｏｘの層についてみると１層分早く解読に有効な性質が壊される。つまり、ある段数のＳＱＵＡＲＥ暗号／Ｒｉｊｎｄａｅｌ暗号に比べて、それより１層分少ない構成でもＳＱＵＡＲＥ攻撃に対する強度は同等と考えられる。よって、ＳＱＵＡＲＥ攻撃に対する安全性は、Ｓ－ｂｏｘ層で１層分は向上していることが分かる。

【０１９６】

次に、図３０～図３４で説明した結合関係については、種々のバリエーションが可能である。以下、この結合関係のバリエーションについて説明する。

【０１９７】

図３０～図３４において例示した大ＭＤＳの構成において、図３７（ａ）に示すように、前段の拡大Ｓ－ｂｏｘ１０３－１－１の後半の４つのＳ－ｂｏｘから取り出した１ビットをそれぞれX_{11}～X_{14}で表し、これらをまとめたものを４ビットデータＸ で表し、同様に、拡大Ｓ－ｂｏｘ１０３－１－２、拡大Ｓ－ｂｏｘ１０３－１－３、拡大Ｓ－ｂｏｘ１０３－１－４、後段の拡大Ｓ－ｂｏｘ１０３－２－１、拡大Ｓ－ｂｏｘ１０３－２－２、拡大Ｓ－ｂｏｘ１０３－２－３、拡大Ｓ－ｂｏｘ１０３－２－４についても、それぞれ、X_{21}～X_{24}およびX_2、X_{31}～X_{34}およびX_3、X_{41}～X_{44}およびX_4、Y_{11}～Y_{14}およびY_1、Y_{21}～

Y_{24}およびY_2、Y_{31}～Y_{34}およびY_3、Y_{41}～Y_{44}およびY_4で表すものとする。

【０１９８】

この場合に、各拡大Ｓ－ｂｏｘ１０３に対応する４ビットデータX_1～X_4、Y_1～Y_4の各々をＧＦ（2^4）の元とみなした場合に、入力側のX_1～X_4から出力側のY_1～Y_4を求めるための大ＭＤＳ行列は、図３７（ｂ）に示すようになる。

【０１９９】

そして、図３０～図３４において、前段の１つの拡大Ｓ－ｂｏｘの後半の４並列のＳ－ｂｏｘから１ビットずつ取り出した４ビットと、後段の１つの拡大Ｓ－ｂｏｘの前半の４並列のＳ－ｂｏｘから１ビットずつ取り出した４ビットとの間の結線（結線パターン）は、図３７（ｂ）に示す対応する行列要素についてのＧＦ（2^4）上の乗算の結線表現（結線パターン）になっている（図３０～図３４において、ｘ５、ｘＡ、ＸＥで示している）。すなわち、図３０～図３４の線形拡散と、図３７（ｂ）の線形拡散は、等価な関係にある。

【０２００】

ここで、図３８に、ＧＦ（2^4）上の乗算の結線表現（結線パターン）を、ＧＦ（2^4）の１～Ｆの元の各々について示す。なお、前述したように、結合部分では、排他的論理和がなされる。

【０２０１】

上記した基準を満たす構成の大ＭＤＳを作成する場合には、図３０～図３４における１６個の結線部分を、図３８の３，６，Ｃ，Ｂ，５，Ａ，７，Ｅに対応する結線表現（結線パターン）のうちから適宜選択して組み合わせて構成することができる。ただし、その逆変換に対応する構成についても、同様の条件が満たされていることが必要である。

【０２０２】

また、この場合に、暗号側の大ＭＤＳ（の候補）を決めた場合の復号側の大ＭＤＳ（の候補）、または逆に復号側の大ＭＤＳ（の候補）を決めた場合の暗号側の大ＭＤＳの（の候補）は、図３７（ｂ）のような行列の逆行列を求めることに

よって、容易に得られる。

【０２０３】

つまり、ＧＦ（2^4）による行列とその逆行列の全ての要素が３，６，Ｃ，Ｂ，５，Ａ，７，Ｅのいずれかであれば、上記した基準を満たすことになる。

【０２０４】

ここで、上記した基準を満たすＭＤＳ行列表現を、図３９（ａ）～（ｄ）、図４０（ａ）～（ｄ）に例示する。

【０２０５】

なお、これら行列の探索は、次の制約の下で行ったものである。

（一）行列は巡回型とする。

（二）要素を並べ替えて一致するものは１個だけ選ぶ。

ここで、並べ替えは、巡回（１，２，３，４）→（２，３，４，１）と、反転（１，２，３，４）→（４，３，２，１）を任意の回数組み合わせてできる操作とする。例えば、（３，３，７，Ｃ）→（３，７，Ｃ，３）→（３，Ｃ，７，３）は該当するが、（３，３，７，Ｃ）→（３，７，３，Ｃ）は該当しない。

また、逆関数の関係にある行列同士を比較すると分かるように、各々の行列は、他の行列の逆行列に並べ替えを行ったものになっている。例えば、（６，Ｂ，Ｅ，Ｅ）は、$(5, 5, A, E)^{-1}$＝（Ｂ，Ｅ，Ｅ，６）を並べ替えたものになっている。

【０２０６】

これら線形拡散は、上記のように対応する乗算の結線表現を用いて図３０～図３４のようにして実回路によって実現することも、行列演算または入出力変換表によっても実現することも可能である。

【０２０７】

図３９（ａ）と（ｂ）とは、逆関数の関係にあり、それらの一方を暗号側に用い、他方を復号側に用いればよく、この点は、図３９（ｃ）と（ｄ）、図４０（ａ）と（ｂ）、図４０（ｃ）と（ｄ）のそれぞれについても、同様である（なお、暗号側と復号側とで、どのような実現方法を採用するかについては、必ずしも揃える必要はない（もちろん、揃えてもよい））。

【０２０８】

ところで、各ｓ－ｂｏｘ間の結線パターンは、図３８の３，６，Ｃ，Ｂ，５，Ａ，７，Ｅに対応するものに限定されず、適宜設定することが可能である。例えば、図４２（ｃ）や（ｄ）に示すような結線パターンは図３８には含まれていないが、これらも使用することが可能である（なお、前述したように、該結線パターンの結合部分では、排他的論理和がなされる）。

【０２０９】

この場合には、図３７（ａ）のX_{11}～X_{14}、X_{21}～X_{24}、X_{31}～X_{34}、X_{41}～X_{44}を１６個の入力とし、Y_{11}～Y_{14}、Y_{21}～Y_{24}、Y_{31}～Y_{34}、Y_{41}～Y_{44}を１６個の出力として、１６行１６列のＭＤＳ行列を用いればよい。

【０２１０】

例えば、図３７（ｂ）の線形拡散は、図４２のように表現することができる。すなわち、図３７（ｂ）の５、ＡまたはＥの要素をそれぞれ対応する４行４列の行列で表現して対応する部分に入れると、図４２のようになる（図４２では、４行４列の部分ごとに区切って記述している）。

【０２１１】

そこで、例えば、あるｓ－ｂｏｘ間の結線パターンとして図４２（ｃ）あるいは（ｄ）に示すような結線パターンを用いる場合には、図３８のような１６行１６列の行列の対応する４行４列の部分を、図４２（ｃ）あるいは（ｄ）に示すような４行４列表現に設定すればよい。他の所望の結線パターンを用いる場合も同様である。なお、結線パターンの４行４列表現は、当該結線パターンの入力側を４つの１ビット入力と、出力側を４つの１ビット出力として考えた場合の変換行列となっているものである。

【０２１２】

このように図３０～図３３のｓ－ｂｏｘ間の結線パターンとして任意の結線パターンを用いる場合にも、暗号側について図４２のように表現した場合の行列の逆行列が、復号側について図４２のように表現した場合の行列となる。また、この場合の線形拡散も、任意の結線パターンを用いて（図３０～図３４と同様にして）実回路によって実現することも、行列演算または入出力変換表によっても実

現することも可能である。

【０２１３】

ところで、上記では基準（１）として、

（１）前段の拡大Ｓ－ｂｏｘの前半における全Ｓ－ｂｏｘのうちから任意に選んだ１つのＳ－ｂｏｘと、後段の拡大Ｓ－ｂｏｘの前半における全Ｓ－ｂｏｘのうちから任意に選んだ１つのＳ－ｂｏｘとが、いずれもの組み合わせについても、２本以上の経路によって相互に接続（結合）されている。

としたが、

この条件を緩和して構成することも可能である。

【０２１４】

例えば、次の条件が考えられる。

（１’）前段の拡大Ｓ－ｂｏｘと後段の拡大Ｓ－ｂｏｘとの全ての組み合わせの各々において、少なくとも１組の、当該前段の拡大Ｓ－ｂｏｘの後半の４つのｓ－ｂｏｘのうちの１つと当該後段の拡大Ｓ－ｂｏｘの前半の４つのｓ－ｂｏｘのうちの１つとが、２本以上の経路によって相互に接続（結合）されている。

また、例えば、次の条件が考えられる。

（１’’）前段の拡大Ｓ－ｂｏｘの前半における少なくとも１つのＳ－ｂｏｘと、後段の拡大Ｓ－ｂｏｘの前半における少なくとも１つのＳ－ｂｏｘとが、２本以上の経路によって相互に接続（結合）されている。

【０２１５】

このような条件の場合には、Ｓ－ｂｏｘ間の結線パターンをＧＦ（2^4）上の乗算の結線表現（結線パターン）に限定するときでも、図３８の１～Ｆに対応する結線表現（結線パターン）のうちから適宜選択して組み合わせて構成することができる。

【０２１６】

また、Ｓ－ｂｏｘ間の結線パターンをＧＦ（2^4）上の乗算の結線表現（結線パターン）に限定しないときは、例えば図４２（ａ）や（ｂ）に例示するものをはじめ様々な結線パターンあるいは対応する行列を用いることができる。

【０２１７】

なお、以上では、暗号側と復号側で同一の基準を適用するものとしたが、暗号側と復号側で異なる基準を採用することも可能である。例えば、暗号側と復号側の一方には上記基準（１）を適用し、他方には上記基準（１’）を適用するこよも可能である。また、その他の適用の仕方も可能である。

【０２１８】

なお、上記と同様の考え方により、８ビット・データのうちの同じ位置の２ビットごとに処理を行うこととして、各要素が８ビットの４行４列のＭＤＳ行列（ＧＦ（2^8））を、４個用意して、大ＭＤＳを構成することも可能である。また、８ビット・データのうちの同じ位置の４ビットごとに処理を行うこととして、各要素が１６ビットの４行４列のＭＤＳ行列（ＧＦ（2^{16}））を、２個用意して、大ＭＤＳを構成することも可能である。また、各要素が３２ビットの４行４列のＭＤＳ行列（ＧＦ（2^{32}））を、１個用意して、大ＭＤＳを構成することも可能である。

【０２１９】

また、以上では、同じ位置のビットを取り出して処理を行うものとして説明したが、異なる位置のビットを（排他的に）取り出して処理を行うことも可能である。

【０２２０】

図４３に、大ＭＤＳの選択手順の一例を示す。

【０２２１】

ここでは、先に暗号側の構成を求めるものとして説明するが、その逆ももちろん可能である（暗号側と復号側が逆になるだけである）。

【０２２２】

まず、ステップＳ１０１で、所定の方法で（例えばランダムに）、暗号側のＭＤＳ行列を求め、ステップＳ１０２で、該行列が一定の基準（例えば、前述した基準（１））を満たしているか否か判定する。一定の基準を満たしていなければ、該行列を破棄し、ステップＳ１０１で他の行列を求める。

【０２２３】

一定の基準を満たした場合には、ステップＳ１０３で、上記ＭＤＳ行列の逆行

列すなわち復号側のＭＤＳ行列を求め、ステップＳ１０４で、該行列が一定の基準（例えば、前述した基準（１））を満たしているか否か判定する。一定の基準を満たしていなければ、これら行列を破棄し、ステップＳ１０１で他の行列を求める。

【０２２４】

一定の基準を満たした場合には、暗号側のＭＤＳ行列および復号側のＭＤＳ行列の組みの候補となる。

【０２２５】

以上の手順を繰り返し行って得た複数の候補のうちから所定の方法で選択したものを採用しても良いし、最初に得られた候補を採用するようにしてもよい。

【０２２６】

なお、大ＭＤＳを実回路で実現する場合には、得られたＭＤＳ行列と等価な結線パターンを用いればよい。

【０２２７】

なお、以上のバリエーションとして、各々の大ＭＤＳの前段及び又は後段に、同一の拡大Ｓ－ｂｏｘに属する複数のＳ－ｂｏｘについてのビットの位置を入れ替える処理を行う（あるいはそのような回路を挿入する）構成も可能である。

【０２２８】

もちろん、ここで説明した大ＭＤＳの構成は、これまで説明してきた種々のバリエーションを持つ暗号化装置や復号装置に適用可能である。

【０２２９】

例えば、上記では、１つの拡張Ｓ－ｂｏｘを４並列２段分の８ビットＳ－ｂｏｘと小ＭＤＳ（と鍵加算）で構成し、このような拡張Ｓ－ｂｏｘを４並列にし、４並列の拡張Ｓ－ｂｏｘと大ＭＤＳとを交互に配置した（４並列の拡張Ｓ－ｂｏｘと４並列の拡張Ｓ－ｂｏｘとを大ＭＤＳで結合した）１２８ビット・ブロック暗号の暗号化装置／復号装置もしくは暗号アルゴリズム／復号アルゴリズムの場合を例にとって説明したが、もちろん、ここで説明した大ＭＤＳの構成は、上記と同様の拡張Ｓ－ｂｏｘを２並列にし、２並列の拡張Ｓ－ｂｏｘと大ＭＤＳとを交互に配置した（２並列の拡張Ｓ－ｂｏｘと２並列の拡張Ｓ－ｂｏｘとを大ＭＤ

Ｓで結合した）６４ビット・ブロック暗号の暗号化装置／復号装置もしくは暗号アルゴリズム／復号アルゴリズムの場合にも適用可能である。

【０２３０】

なお、このような６４ビット・ブロック暗号の場合、１２８ビット・ブロック暗号の構成における４並列の拡張Ｓ－ｂｏｘの部分を２並列の拡張Ｓ－ｂｏｘに置き換えるとともに、これに対応する部分を修正すればよい。

【０２３１】

例えば、鍵長は、１２８ビットとすればよいし、もちろん、６４ビットや９６ビットなど、他の鍵長も可能である。なお、この場合の段数Ｒは、好ましくは６段以上とする。

【０２３２】

６４ビット・ブロック暗号の場合、図３０～図３４の構成では、４並列の拡張Ｓ－ｂｏｘが２並列の拡張Ｓ－ｂｏｘになる点が異なるが、前述した基準や結合の方法や結合パターンは同様である。また、図３７（ｂ）や図３９や図４０の大ＭＤＳ行列は、２行２列になる。また、これに対応して、図４１の大ＭＤＳ行列は、８行８列になる。なお、拡張Ｓ－ｂｏｘの内部構成は同じであるので、図３８や図４２などの結合パターンは同じものが使用可能である。また、図４３の手順も同様である。

【０２３３】

ブロックデータがその他のデータ長の場合ももちろん可能である。

【０２３４】

また、拡張Ｓ－ｂｏｘ内のＳ－ｂｏｘの並列数が異なる場合ももちろん可能である。

【０２３５】

上記のような大ＭＤＳを用いた１２８ビット暗号の場合の一構成例に係る共通鍵ブロック暗号方式による暗号化装置あるいは復号装置は、例えば、初段では入力された１２８ビットの平文ブロックデータを、２段目以降では前段での処理が施された１２８ビットのブロックデータを入力とし、該ブロックデータを４分割した４組の３２ビット・データに対してそれぞれ局所的な線形拡散処理および非

線形変換処理を施し出力する４つの第１の非線形変換処理部と、これら４つの第１の非線形変換処理部からそれぞれ出力された４組の３２ビット・データを連結した１２８ビットのブロックデータに対して最大距離分離行列を用いて線形拡散処理を施し次段へ出力する第１の拡散処理部とを、１段分の段構成として、該段構成を所定段数分接続し、最後の前記第１の拡散処理部の後段に、この第１の拡散処理部から出力される１２８ビットのブロックデータを入力とする前記４つの第１の非線形変換処理部を接続し、この４つの第１の非線形変換処理部の後段に、これら４つの第１の非線形変換処理部からそれぞれ出力された４組の３２ビット・データを連結した１２８ビットのブロックデータに対して１２８ビットの鍵データを加算して１２８ビットの暗号化されたブロックデータとして出力する第１の鍵加算部を接続して構成されるとともに、前記第１の非線形変換処理部の各々は、与えられた１組の前記３２ビット・データをさらに４分割した４組の８ビット・データに対してそれぞれ８ビットの鍵データを加算する４つの第２の鍵加算部と、各第２の鍵加算部の出力に対してそれぞれ８ビットの入出力変換表を用いて非線形変換を行う４つの第２の非線形変換処理部と、これら４つの第２の非線形変換処理部からそれぞれ出力された４組の８ビット・データを連結した３２ビット・データに対して最大距離分離行列を用いて線形拡散処理を施す第２の拡散処理部と、この第２の拡散処理部の後段にさらに接続された４組の前記第２の鍵加算部および第２の非線形変換処理部とを含むものであり、前記第１の拡散処理部の各々は、前段の１つの第１の非線形変換処理部の４つの第２の非線形変換処理部からそれぞれ出力される８ビットのうちの相対応する１ビットを一纏めにした４ビットを行列演算における入力側の１つの要素とするとともに、後段の１つの第１の非線形変換処理部の４つの第２の非線形変換処理部へそれぞれ入力される８ビットのうちの相対応する１ビットを一纏めにした４ビットを行列演算における出力側の１つの要素として、2^4のガロア体の乗算に基づいた４行４列の行列演算またはこれと等価な回路によって線形拡散処理を行う１６ビット拡散手段を、該前段及び後段の第２の非線形変換処理部についての該８ビットのうちの各ビットに対応して有し、１つの前記１６ビット拡散手段における前記2^4のガロア体の乗算に基づいた４行４列の行列演算またはこれと等価な回路では、前段

の４つの第１の非線形変換処理手段の最終段における合計１６の第２の非線形変換処理手段からの出力となる任意の１ビットと、後段の４つの第１の非線形変換処理手段の初段における合計１６の第２の非線形変換処理手段へ入力となる任意の１ビットとのすべての組み合わせにおいて、前段側における当該１ビットの状態を、後段側における当該１ビットへ、複数の演算経路を辿って波及させるための手段を含むものである。

【０２３６】

また、上記のような大ＭＤＳを用いた６４ビット暗号の場合の一構成例に係る共通鍵ブロック暗号方式による暗号化装置あるいは復号装置は、例えば、初段では入力された６４ビットの平文ブロックデータを、２段目以降では前段での処理が施された６４ビットのブロックデータを入力とし、該ブロックデータを２分割した２組の３２ビット・データに対してそれぞれ局所的な線形拡散処理および非線形変換処理を施し出力する２つの第１の非線形変換処理部と、これら２つの第１の非線形変換処理部からそれぞれ出力された２組の３２ビット・データを連結した６４ビットのブロックデータに対して最大距離分離行列を用いて線形拡散処理を施し次段へ出力する第１の拡散処理部とを、１段分の段構成として、該段構成を所定段数分接続し、最後の前記第１の拡散処理部の後段に、この第１の拡散処理部から出力される６４ビットのブロックデータを入力とする前記２つの第１の非線形変換処理部を接続し、この２つの第１の非線形変換処理部の後段に、これら２つの第１の非線形変換処理部からそれぞれ出力された２組の３２ビット・データを連結した６４ビットのブロックデータに対して６４ビットの鍵データを加算して６４ビットの暗号化されたブロックデータとして出力する第１の鍵加算部を接続して構成されるとともに、前記第１の非線形変換処理部の各々は、与えられた１組の前記３２ビット・データをさらに４分割した４組の８ビット・データに対してそれぞれ８ビットの鍵データを加算する４つの第２の鍵加算部と、各第２の鍵加算部の出力に対してそれぞれ８ビットの入出力変換表を用いて非線形変換を行う４つの第２の非線形変換処理部と、これら４つの第２の非線形変換処理部からそれぞれ出力された４組の８ビット・データを連結した３２ビット・データに対して最大距離分離行列を用いて線形拡散処理を施す第２の拡散処理部と

、この第２の拡散処理部の後段にさらに接続された４組の前記第２の鍵加算部および第２の非線形変換処理部とを含むものであり、前記第１の拡散処理部の各々は、前段の１つの第１の非線形変換処理部の４つの第２の非線形変換処理部からそれぞれ出力される８ビットのうちの相対応する１ビットを一纏めにした４ビットを行列演算における入力側の１つの要素とするとともに、後段の１つの第１の非線形変換処理部の４つの第２の非線形変換処理部へそれぞれ入力される８ビットのうちの相対応する１ビットを一纏めにした４ビットを行列演算における出力側の１つの要素として、2^4のガロア体の乗算に基づいた２行２列の行列演算またはこれと等価な回路によって線形拡散処理を行う８ビット拡散手段を、該前段及び後段の第２の非線形変換処理部についての該８ビットのうちの各ビットに対応して有し、１つの前記８ビット拡散手段における前記2^4のガロア体の乗算に基づいた２行２列の行列演算またはこれと等価な回路では、前段の２つの第１の非線形変換処理手段の最終段における合計８の第２の非線形変換処理手段からの出力となる任意の１ビットと、後段の２つの第１の非線形変換処理手段の初段における合計８の第２の非線形変換処理手段へ入力となる任意の１ビットとのすべての組み合わせにおいて、前段側における当該１ビットの状態を、後段側における当該１ビットへ、複数の演算経路を辿って波及させるための手段を含むものである。

【０２３７】

以下では、本実施形態のハードウェア構成、ソフトウェア構成について説明する。

【０２３８】

本実施形態の暗号化装置や復号装置は、ハードウェアとしても、ソフトウェアとしても、実現可能である。

【０２３９】

本実施形態は、ソフトウェアで実現する場合に、暗号化装置や復号装置を実現するプログラムであって、コンピュータに所定の手段を実行させるための（あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための）プログラムを記録したコンピュータ読取り可

能な記録媒体としても実施することもできる。

【０２４０】

また、ハードウェアとして構成する場合、半導体装置として形成することができる。

【０２４１】

また、本発明を適用した暗号化装置や復号装置を構成する場合、あるいは暗号化プログラムや復号プログラムを作成する場合に、図４や図２４で例示したようなブロックもしくはモジュールをすべて個別に作成することも可能であるが、同一構成を有するブロックもしくはモジュールについては１または適当数のみ用意しておいて、それをアルゴリズムの各部分で共有する（使い回す）ことも可能である。

【０２４２】

また、ソフトウェアの場合には、マルチプロセッサを利用し、並列処理を行って、処理を高速化することも可能である。

【０２４３】

なお、暗号化機能を持ち、復号機能を持たない装置として構成することも、復号機能を持ち、暗号化機能を持たない装置として構成することも、暗号化機能と復号機能の両方を持つ装置として構成することも、可能である。同様に、暗号化機能を持ち、復号機能を持たないプログラムとして構成することも、復号機能を持ち、暗号化機能を持たないプログラムとして構成することも、暗号化機能と復号機能の両方を持つプログラムとして構成することも、可能である。

【０２４４】

次に、本実施形態のシステムへの応用について説明する。

【０２４５】

本実施形態の暗号方式は、基本的にはどのようなシステムにも適用可能である。

【０２４６】

例えば、図４４に示すように、送信側装置３０１と、受信側装置３０３との間で、所定の方法もしくは手続により、鍵を安全に共有しておき、送信側装置３０

１は送信データをブロック長ごとに本実施形態の暗号方式で暗号化し、所定のプロトコルに従って、通信ネットワーク３０２を介して、暗号文を受信側装置３０３へ送信し、暗号文を受信した受信側装置３０３では、受信した暗号文をブロック長ごとに本実施形態の暗号方式で復号し、もとの平文を得ることができる。なお、各々の装置が、暗号化機能と復号機能を両方持っていれば、双方向に暗号通信を行うことができる。

【０２４７】

また、例えば、図４５に示すように、計算機３１１では、所定の方法で鍵を生成し、保存したいデータをブロック長ごとに本実施形態の暗号方式で暗号化し、所定のネットワーク（例えば、ＬＡＮ、インターネット等）３１４を介して、暗号化データとして、データ・サーバ３１３に保存しておく。計算機３１１では、このデータを読みたいときは、データ・サーバ３１３から所望の暗号化データを読み込み、これをブロック長ごとに本実施形態の暗号方式で復号し、もとの平文を得ることができる。また、他の計算機３１２が、この鍵を知っていれば、同様に復号してもとの平文を得ることができるが、鍵の分からない他の計算機は、該暗号データを復号することはできず、情報のセキュリティ・コントロールが可能になる。

【０２４８】

また、例えば、図４６に示すように、コンテンツ提供側では、暗号化装置３２１により、あるコンテンツを、ある鍵で、ブロック長ごとに本実施形態の暗号方式で暗号化し、これを暗号化コンテンツとして、記録媒体３２２に記録し、これを頒布等する。記録媒体３２２を取得したユーザ側では、所定の方法で該ある鍵を入手することにより、復号装置３２３により、該コンテンツを、ブロック長ごとに本実施形態の暗号方式で復号し、コンテンツの閲覧もしくは再生等を行うことができる。

【０２４９】

もちろん、上記以外にも種々のシステムに適用可能である。

【０２５０】

なお、本実施形態で示した各々の構成は、一例であって、それ以外の構成を排

除する趣旨のものではなく、例示した構成の一部を他のもので置き換えたり、例示した構成の一部を省いたり、例示した構成に別の機能を付加したり、それらを組み合わせたりすることなどによって得られる別の構成も可能である。また、例示した構成と論理的に等価な別の構成、例示した構成と論理的に等価な部分を含む別の構成、例示した構成の要部と論理的に等価な別の構成なども可能である。また、例示した構成と同一もしくは類似の目的を達成する別の構成、例示した構成と同一もしくは類似の効果を奏する別の構成なども可能である。

また、各種構成部分についての各種バリエーションは、適宜組み合わせて実施することが可能である。

また、本実施形態は、暗号化装置としての発明、復号化装置としての発明、システム全体としての発明、個別装置内部の構成部分についての発明、またはそれらに対応する方法の発明等、種々の観点、段階、概念またはカテゴリに係る発明を包含・内在するものである。

従って、この発明の実施の形態に開示した内容からは、例示した構成に限定されることなく発明を抽出することができるものである。

【０２５１】

本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【０２５２】

【発明の効果】

本発明によれば、局所的なデータ拡散を行う小型の拡散層とブロック幅に及ぶ拡散を行う大型の拡散層を交互に重ねて運用することにより、計算コストを抑えたまま高く均一な拡散を実現することができる。

【図面の簡単な説明】

【図１】

本発明の一実施形態に係る暗号方式の基本的な構成について説明するための図

【図２】

同実施形態の暗号強度に関して説明するための図

【図３】

同実施形態の入れ子型暗号方式のデータ攪拌部の階層構造の例を示す図

【図４】

同実施形態の暗号化装置の構成例を示す図

【図５】

同実施形態のＳ－ｂｏｘの一例を示す図

【図６】

同実施形態の拡大Ｓ－ｂｏｘの内部構成例を示す図

【図７】

同実施形態の小ＭＤＳの一例を示す図

【図８】

同実施形態の大ＭＤＳおよび拡大Ｓ－ｂｏｘの構造例を示す図

【図９】

同実施形態の大ＭＤＳの一例を示す図

【図１０】

同実施形態の大ＭＤＳの他の例を示す図

【図１１】

同実施形態の鍵スケジュール部の構成例を示す図

【図１２】

同実施形態の鍵スケジュール部の他の構成例を示す図

【図１３】

同実施形態の非線形変換層の内部構成の一例を示す図

【図１４】

同実施形態の非線形変換層の内部構成の他の例を示す図

【図１５】

同実施形態の加算定数表の一例を示す図

【図１６】

同実施形態の有限体乗算装置の構成例を示す図

【図１７】

同実施形態の線形変換装置の構成例を示す図

【図１８】

同実施形態の線形変換装置の構成例を示す図

【図１９】

同実施形態のＭＤＳ行列生成装置の構成例を示す図

【図２０】

同実施形態のＭＤＳ行列生成処理手順の一例を示すフローチャート

【図２１】

同実施形態のＭＤＳ行列生成装置の他の構成例を示す図

【図２２】

同実施形態のＭＤＳ行列生成処理手順の他の例を示すフローチャート

【図２３】

同実施形態のＳ－ｂｏｘと小ＭＤＳの組み合わせを選択するための処理手順の一例を示すフローチャート

【図２４】

同実施形態の復号装置の構成例を示す図

【図２５】

同実施形態の拡大Ｓ－ｂｏｘの内部構成例を示す図

【図２６】

同実施形態の大ＭＤＳおよび拡大Ｓ－ｂｏｘの構造例を示す図

【図２７】

同実施形態の鍵スケジュール部の構成例を示す図

【図２８】

同実施形態の大ＭＤＳのさらに他の例を示す図

【図２９】

同実施形態の大ＭＤＳのさらに他の例を示す図

【図３０】

同実施形態の大ＭＤＳのＳ－ｂｏｘ間の結線パターンの一例を示す図

【図３１】

同実施形態の大ＭＤＳのＳ－ｂｏｘ間の結線パターンの一例を示す図

【図３２】

同実施形態の大ＭＤＳのＳ－ｂｏｘ間の結線パターンの一例を示す図

【図３３】

同実施形態の大ＭＤＳのＳ－ｂｏｘ間の結線パターンの一例を示す図

【図３４】

同実施形態の大ＭＤＳのＳ－ｂｏｘ間の結線パターンの一例を示す図

【図３５】

同実施形態の大ＭＤＳの前段と後段のＳ－ｂｏｘ間の経路について説明するための図

【図３６】

従来の隣接する段のＳ－ｂｏｘ間の経路について説明するための図

【図３７】

同実施形態の大ＭＤＳのＧＦ（2^4）による行列表現について説明するための図

【図３８】

ＧＦ（2^4）上の乗算の結線表現を示す図

【図３９】

ファン・インに関する基準（１）を満たすＭＤＳ行列の例を示す図

【図４０】

ファン・インに関する基準（１）を満たすＭＤＳ行列の例を示す図

【図４１】

同実施形態の大ＭＤＳの１６行１６列の行列表現について説明するための図

【図４２】

ＧＦ（2^4）上の乗算の結線表現以外の結線表現の例を示す図

【図４３】

同実施形態の大ＭＤＳ行列選択処理手順の一例を示すフローチャート

【図４４】

同実施形態の暗号方式を利用したシステムの一例を示す図

【図４５】

同実施形態の暗号方式を利用したシステムの他の例を示す図

【図４６】

同実施形態の暗号方式を利用したシステムのさらに他の例を示す図

【符号の説明】

１…暗号処理装置

２…最上位の階層の非線形変換モジュール

３…データ幅に渡る拡散モジュール

４…階層構造内部の非線形変換モジュール

５…局所的な拡散モジュール

１０２…拡大Ｓ－ｂｏｘ層

１０３，１１０３…拡大Ｓ－ｂｏｘ

１０４，１３１，１１０４…大ＭＤＳ

１０５，１１０５…（暗号文直前の）鍵加算部

１１１，１１１１…鍵加算部

１１２，１４１，１１１２…Ｓ－ｂｏｘ

１１３，１４２，１１１３…小ＭＤＳ

１２１～１２４…鍵スケジュール部

１３４，１４３…排他的論理和部

１３５，１３６…剰余加算部

２００…有限体乗算装置

２０１…桁溢れ帰還部

２０２…係数格納部

２０３…乗算部

２０４，２０５…排他的論理和部

２３１…要素生成部

２３２…小行列式計算部

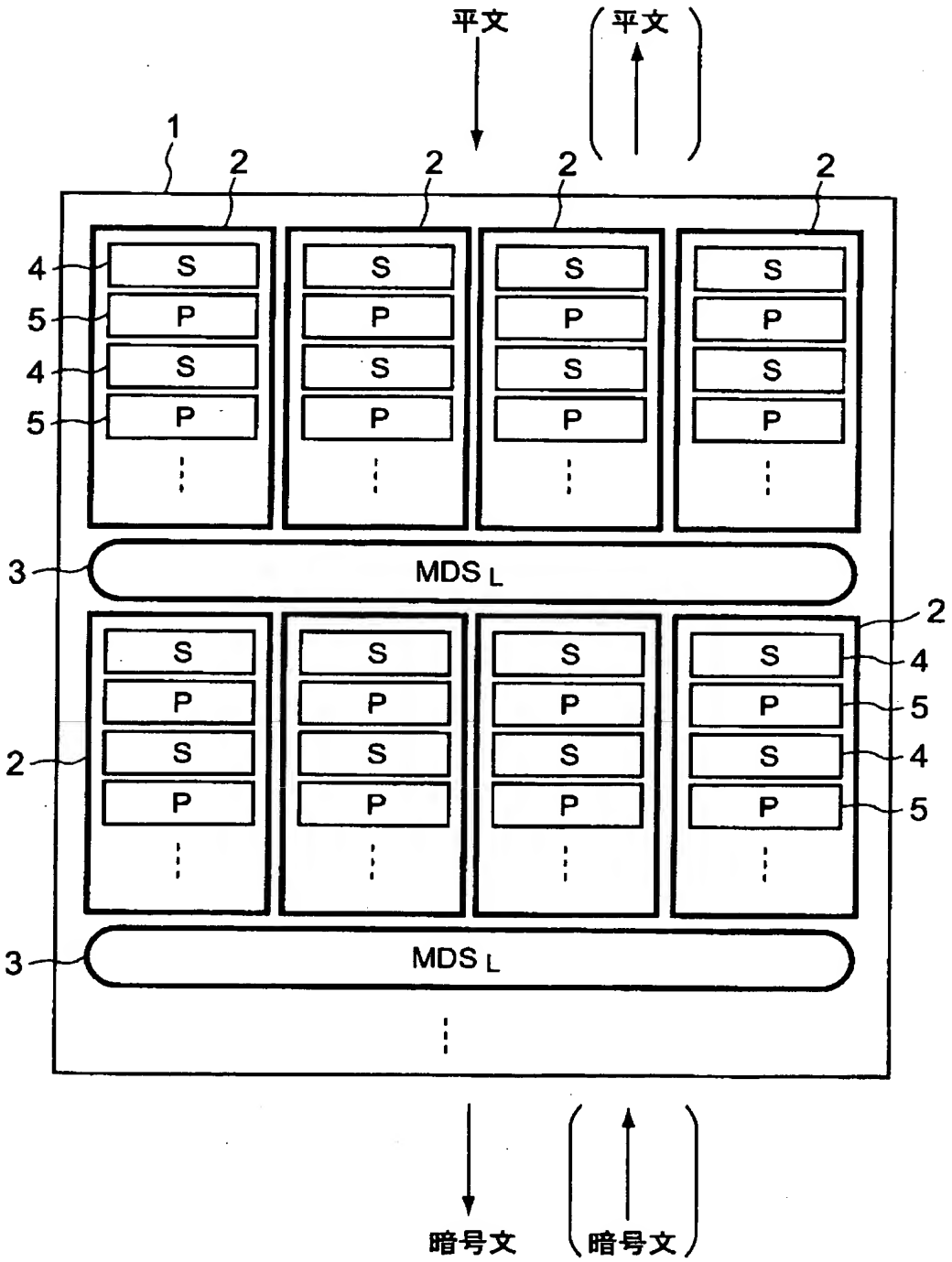
２３３…判定部

２３４…逆行列生成部

２３５…逆行列判定部

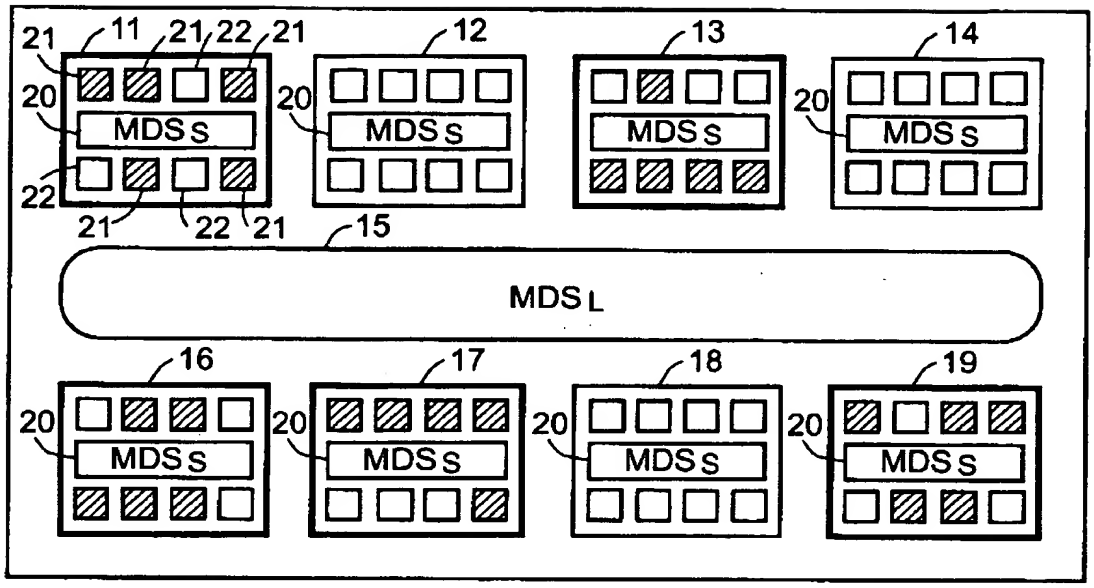
【書類名】　　図面

【図１】

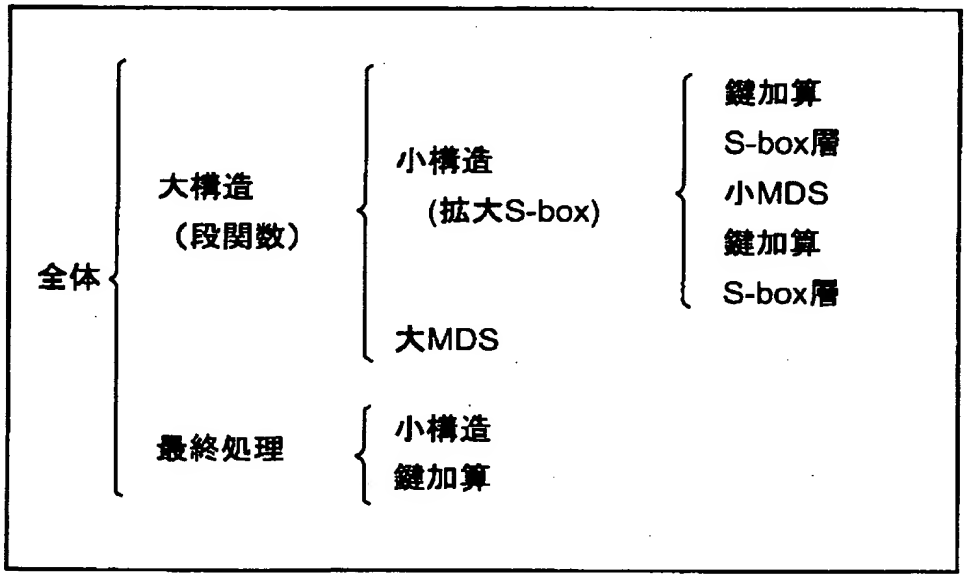


出証特２００１－３０５０９３８

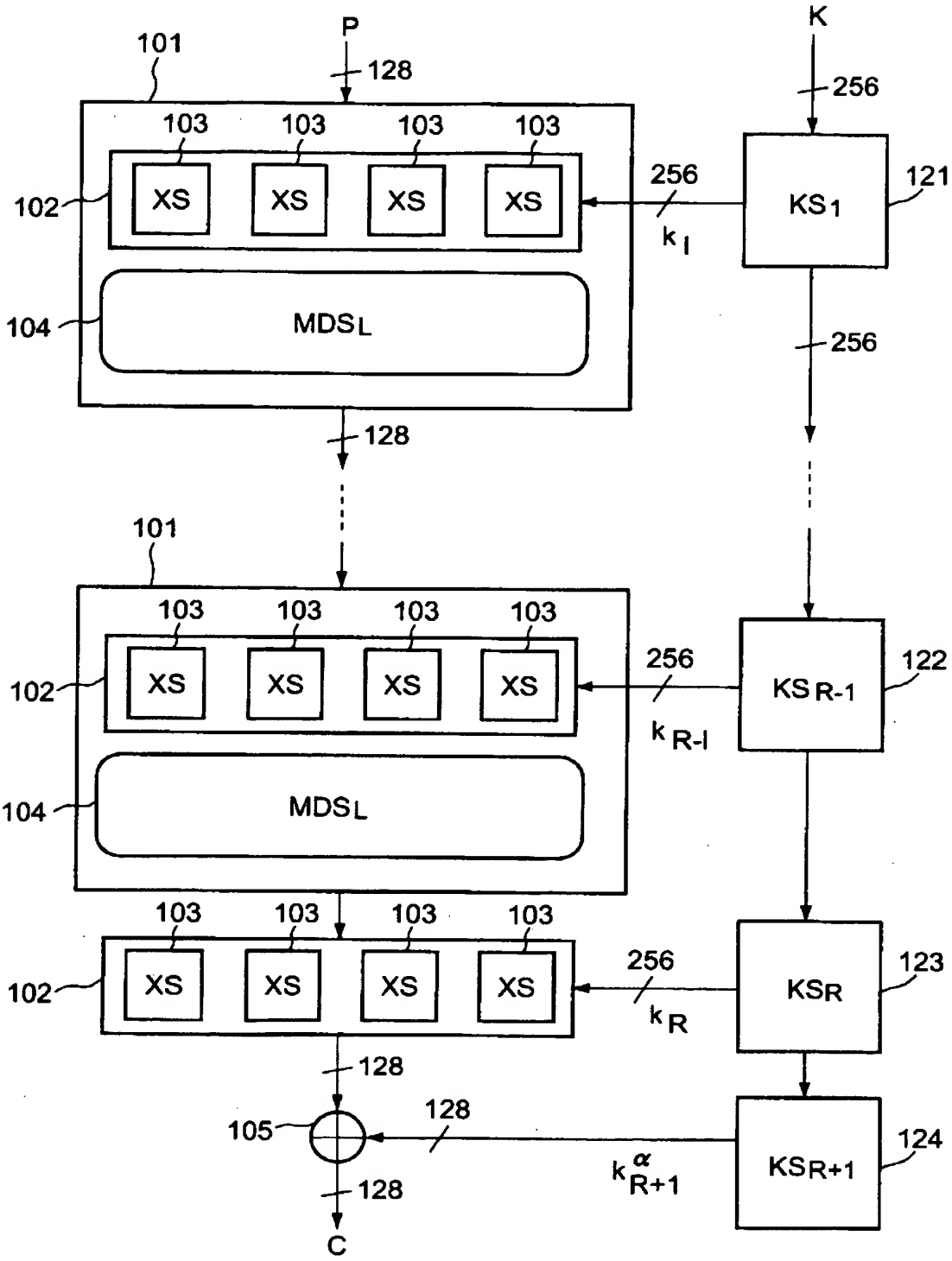
【図２】


21
11
21
22
21
12
13
14
20
MDSS
22
21
22
21
15
MDSL
16
17
18
19

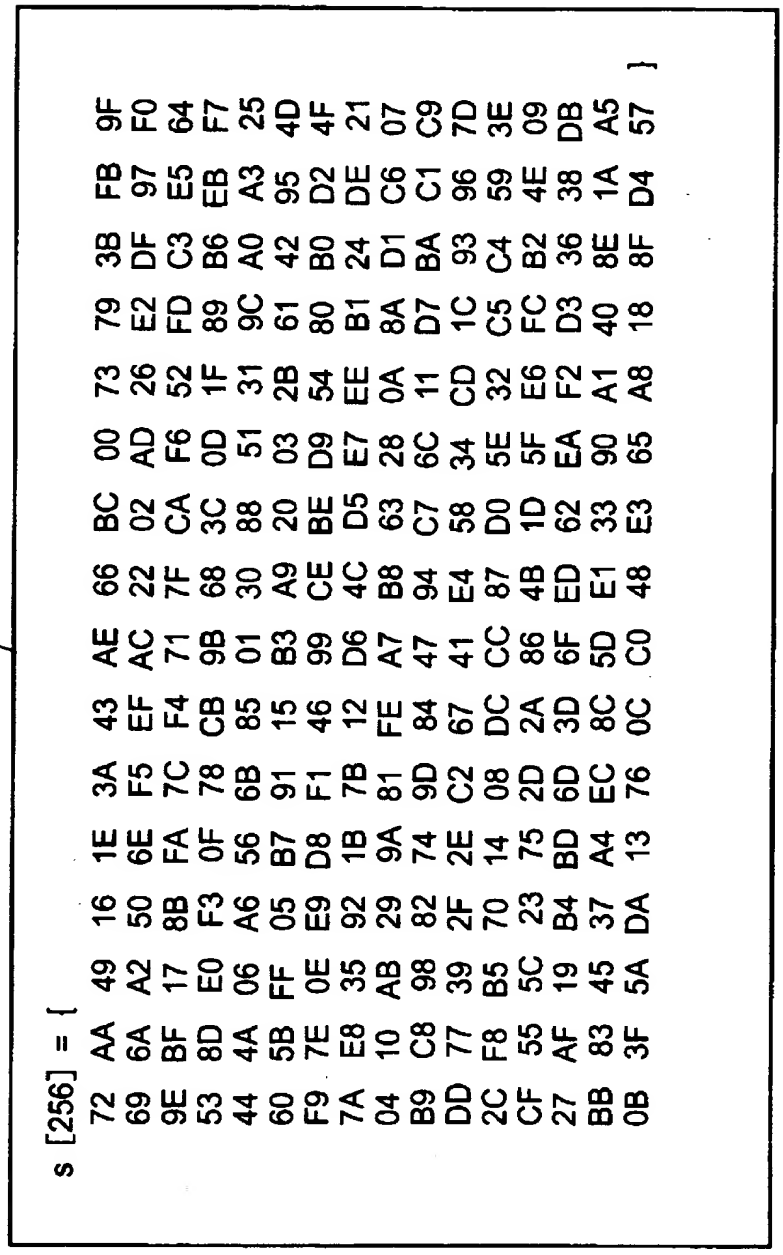
【図３】


全体
大構造
（段関数）
小構造
（拡大S-box)
鍵加算
S-box層
小MDS
鍵加算
S-box層
大MDS
最終処理
小構造
鍵加算

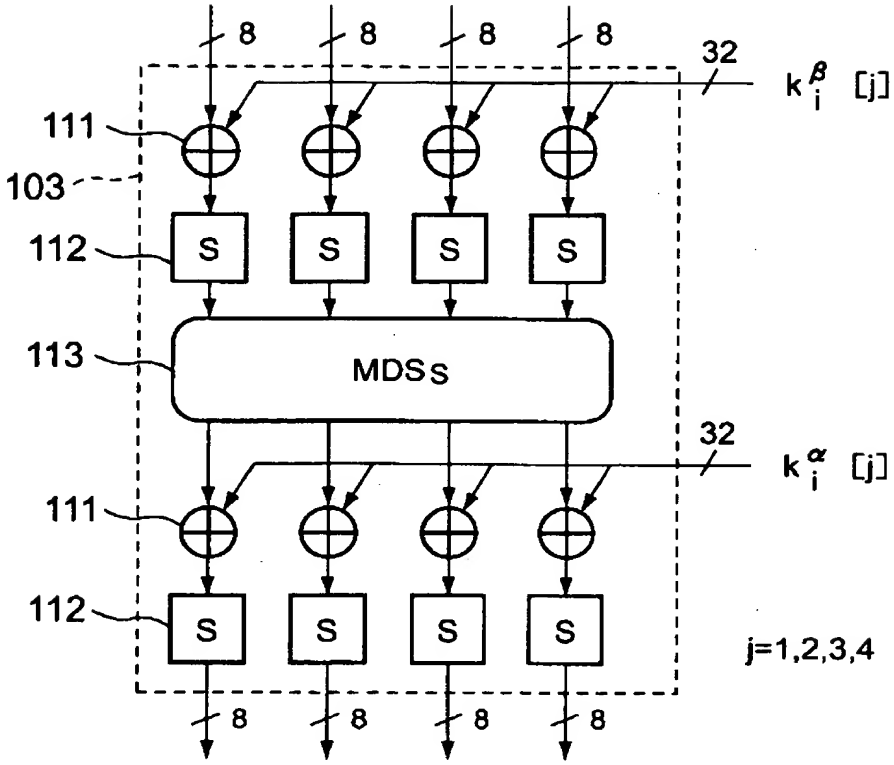
【図４】


P
128
101
K
256
103
103
103
103
XS
XS
XS
XS
102
256
k_I
KS_1
121
104
MDS_L
256
128
101
103
103
103
103
XS
XS
XS
XS
102
256
k_{R-I}
KS_{R-1}
122
104
MDS_L
103
103
103
103
XS
XS
XS
XS
102
256
k_R
KS_R
123
128
105
128
k^{α}_{R+1}
KS_{R+1}
124
128
C

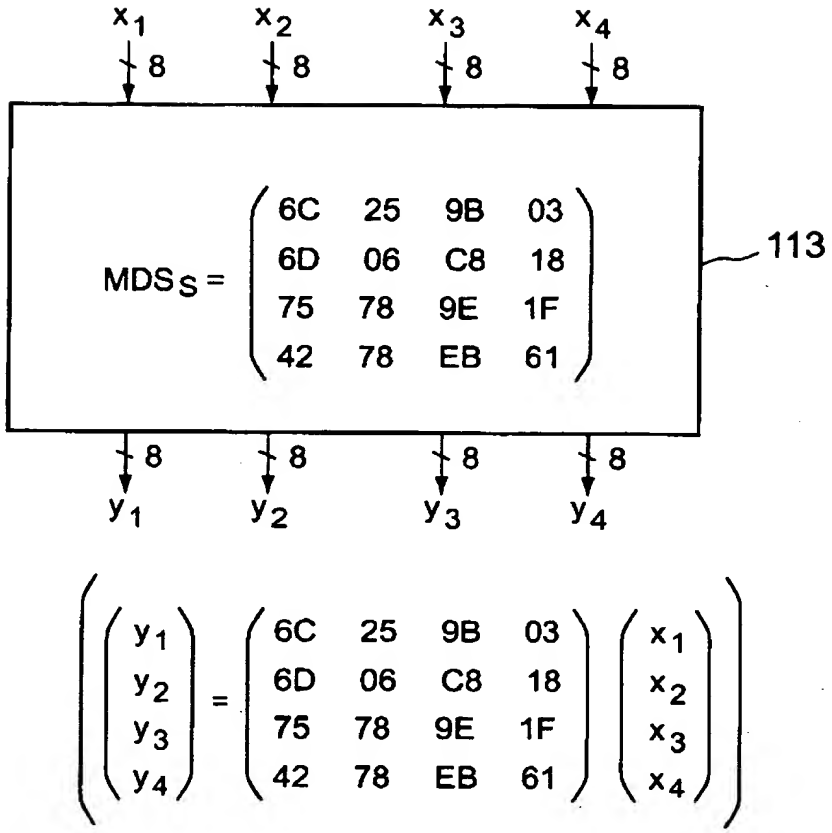
【図５】


112
s [256] = {
72 AA 49 16 1E 3A 43 AE 66 BC 00 73 79 3B FB 9F
69 6A A2 50 6E F5 EF AC 22 02 AD 26 E2 DF 97 F0
9E BF 17 8B FA 7C F4 71 7F CA F6 52 FD C3 E5 64
53 8D E0 F3 0F 78 CB 9B 68 3C 0D 1F 89 B6 EB F7
44 4A 06 A6 56 6B 85 01 30 88 51 31 9C A0 A3 25
60 5B FF 05 B7 91 15 B3 A9 20 03 2B 61 42 95 4D
F9 7E 0E E9 D8 F1 46 99 CE BE D9 54 80 B0 D2 4F
7A E8 35 92 1B 7B 12 D6 4C D5 E7 EE B1 24 DE 21
04 10 AB 29 9A 81 FE A7 B8 63 28 0A 8A D1 C6 07
B9 C8 98 82 74 9D 84 47 94 C7 6C 11 D7 BA C1 C9
DD 77 39 2F 2E C2 67 41 E4 58 34 CD 1C 93 96 7D
2C F8 B5 70 14 08 DC CC 87 D0 5E 32 C5 C4 59 3E
CF 55 5C 23 75 2D 2A 86 4B 1D 5F E6 FC B2 4E 09
27 AF 19 B4 BD 6D 3D 6F ED 62 EA F2 D3 36 38 DB
BB 83 45 37 A4 EC 8C 5D E1 33 90 A1 40 8E 1A A5
0B 3F 5A DA 13 76 0C C0 48 E3 65 A8 18 8F D4 57 }

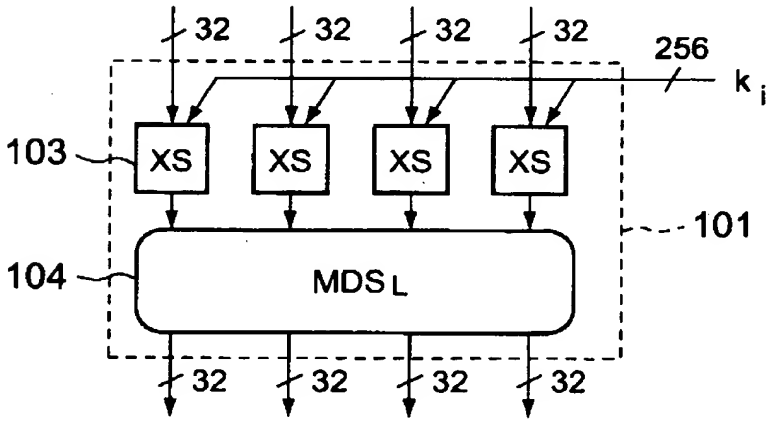
【図６】


8
8
8
8
32
k_i^{β} [j]
111
103
112
S
S
S
S
113
MDSS
32
k_i^{α} [j]
111
112
S
S
S
S
j=1,2,3,4
8
8
8
8

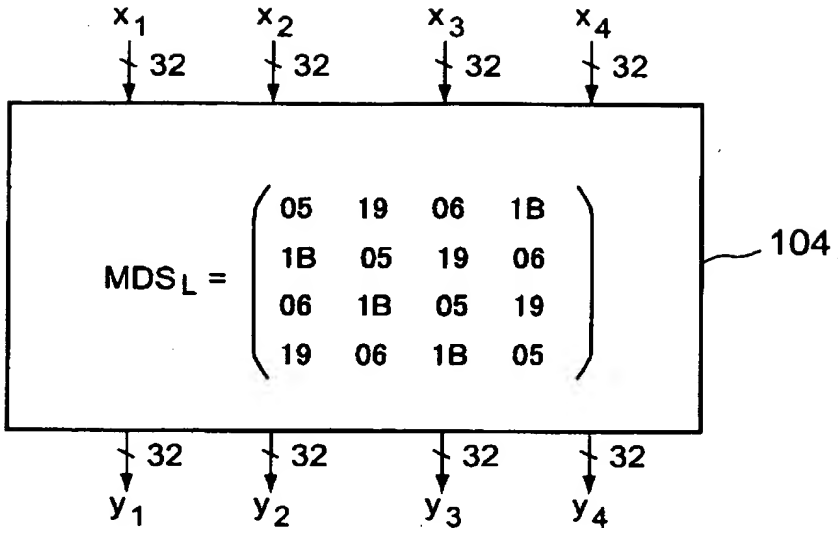
【図７】


x1
x2
x3
x4
8
8
8
8
MDSS =
6C 25 9B 03
6D 06 C8 18
75 78 9E 1F
42 78 EB 61
113
8
8
8
8
y1
y2
y3
y4
y1 y2 y3 y4 = 6C 25 9B 03 / 6D 06 C8 18 / 75 78 9E 1F / 42 78 EB 61 x1 x2 x3 x4

【図８】

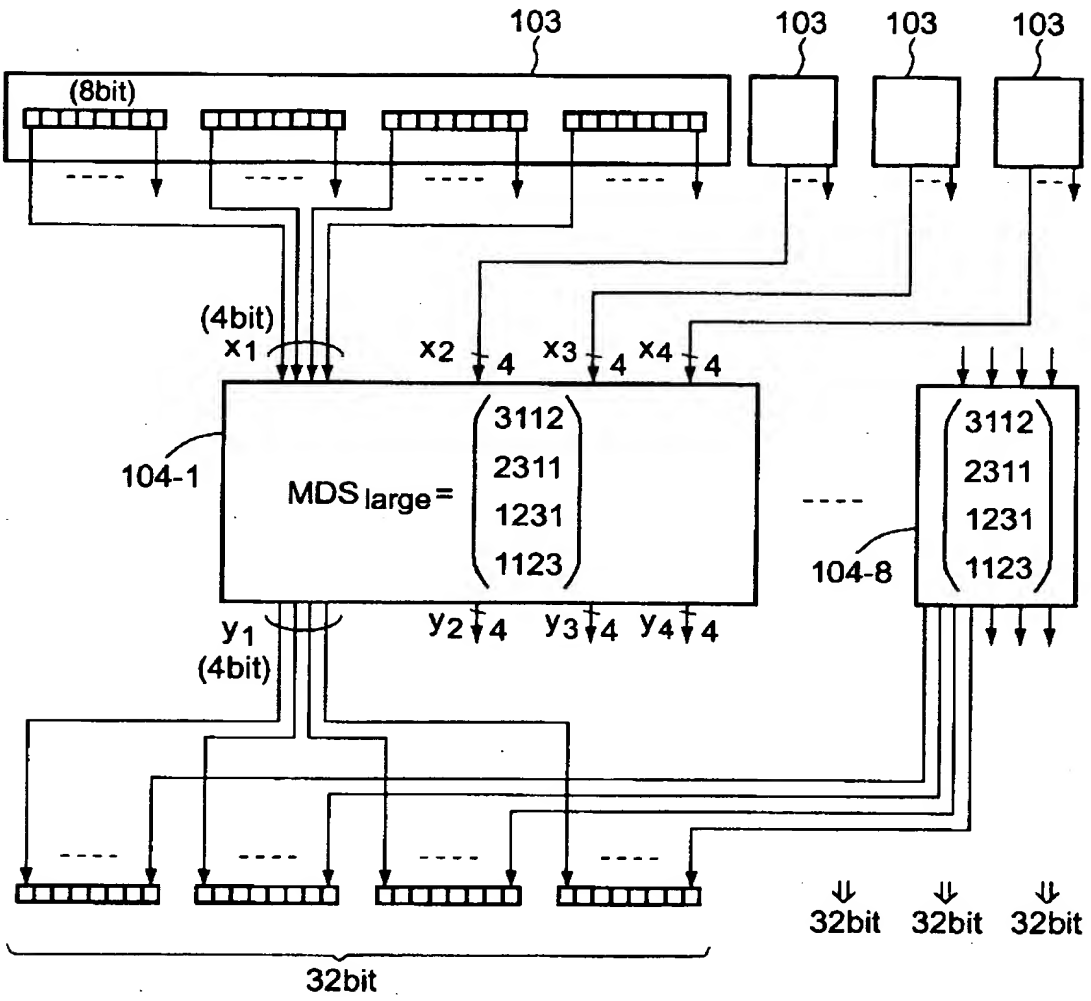

32
32
32
32
256
ki
103
XS
XS
XS
XS
101
104
MDSL
32
32
32
32

【図９】



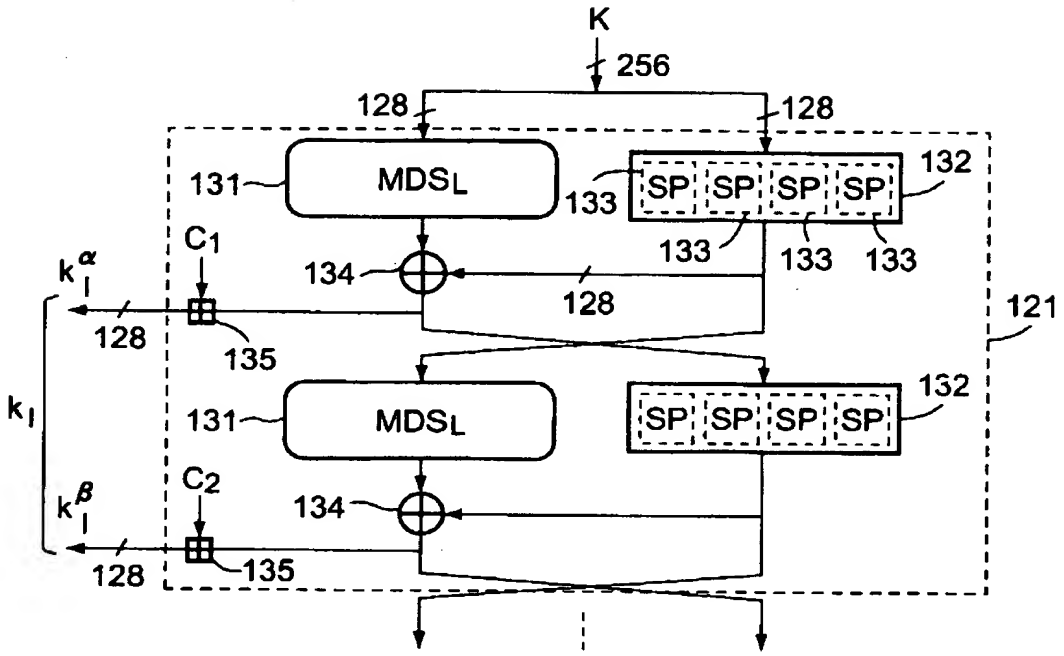
$$\left(\begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} 05 & 19 & 06 & 1B \\ 1B & 05 & 19 & 06 \\ 06 & 1B & 05 & 19 \\ 19 & 06 & 1B & 05 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \right)$$

【図１０】

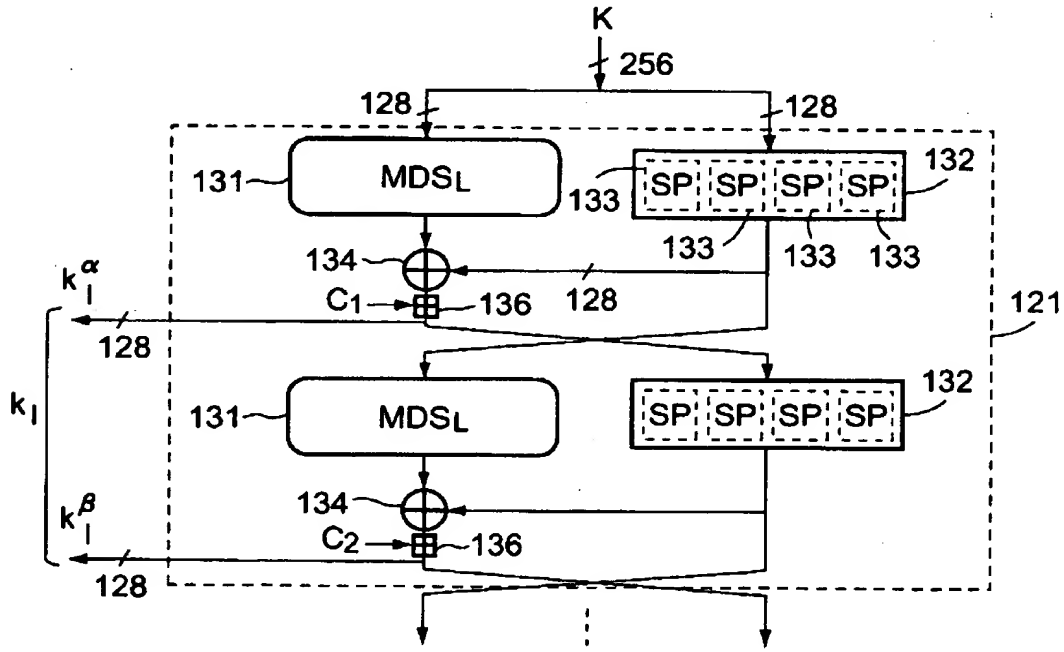


$$\left(\begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} 3112 \\ 2311 \\ 1231 \\ 1123 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \right)$$

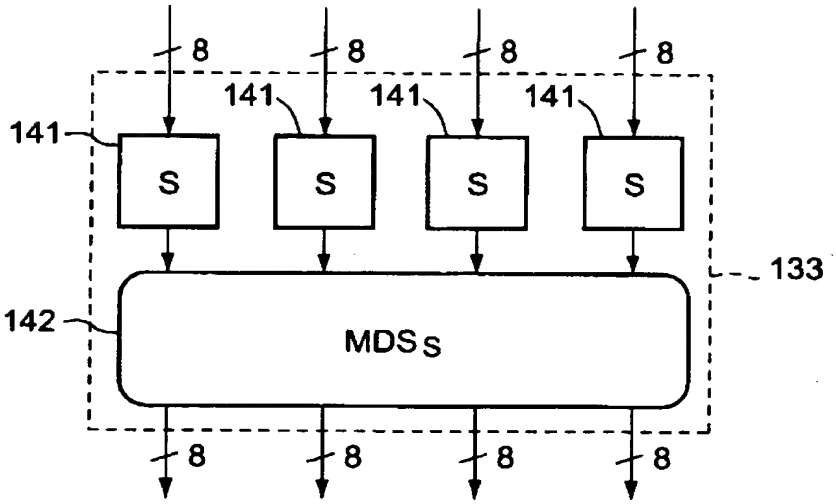
【図１１】


K
256
128
128
131
MDSL
133
SP
SP
SP
SP
132
133
133
133
C1
134
128
121
kα l
128
135
kl
131
MDSL
SP
SP
SP
SP
132
C2
134
kβ l
128
135

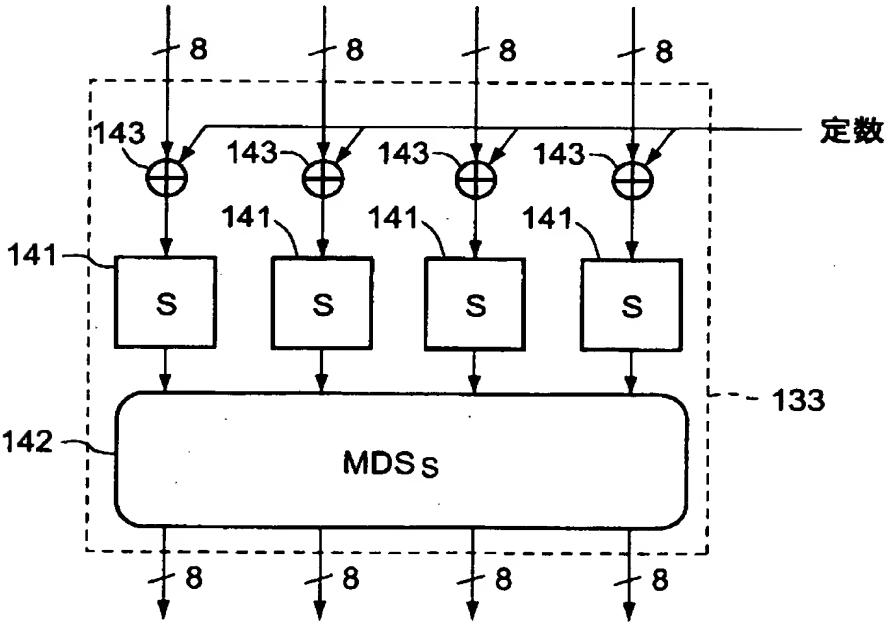
【図１２】


K
256
128
128
131
MDSL
133
SP
SP
SP
SP
132
133
133
133
134
C1
136
128
121
kα l
128
kl
131
MDSL
SP
SP
SP
SP
132
134
C2
136
kβ l
128

【図１３】


8
8
8
8
141
141
141
141
S
S
S
S
133
142
MDS S
8
8
8
8

【図１４】


8
8
8
8
143
143
143
143
定数
141
141
141
141
S
S
S
S
133
142
MDS S
8
8
8
8

【図１５】

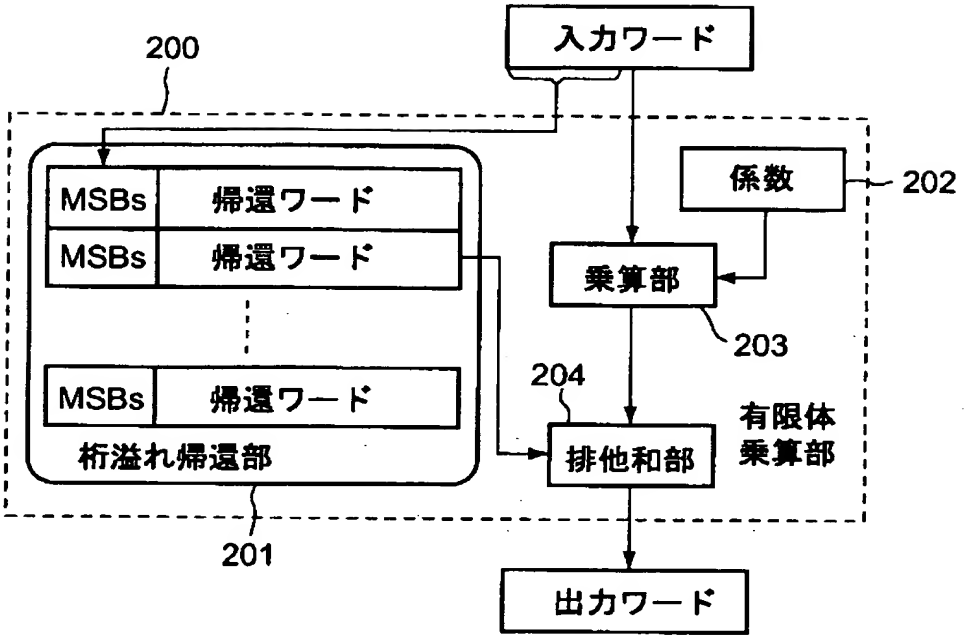
(a)

C_1	(H_2, H_0, H_1, H_1)
C_2	(H_3, H_2, H_0, H_3)
C_3	(H_1, H_0, H_0, H_0)
C_4	(H_1, H_0, H_1, H_3)
C_5	(H_0, H_1, H_0, H_2)
C_6	(H_3, H_2, H_0, H_0)
C_7	(H_1, H_2, H_1, H_0)
C_8	(H_2, H_1, H_2, H_3)
C_9	(H_2, H_1, H_0, H_0)
C_{10}	(H_1, H_1, H_1, H_2)
C_{11}	(H_3, H_1, H_1, H_2)
C_{12}	(H_1, H_1, H_2, H_0)
C_{13}	(H_1, H_3, H_3, H_1)
C_{14}	(H_2, H_3, H_3, H_1)
C_{15}	(H_1, H_3, H_1, H_0)
C_{16}	(H_1, H_0, H_0, H_3)
C_{17}	(H_1, H_2, H_0, H_3)

(b)

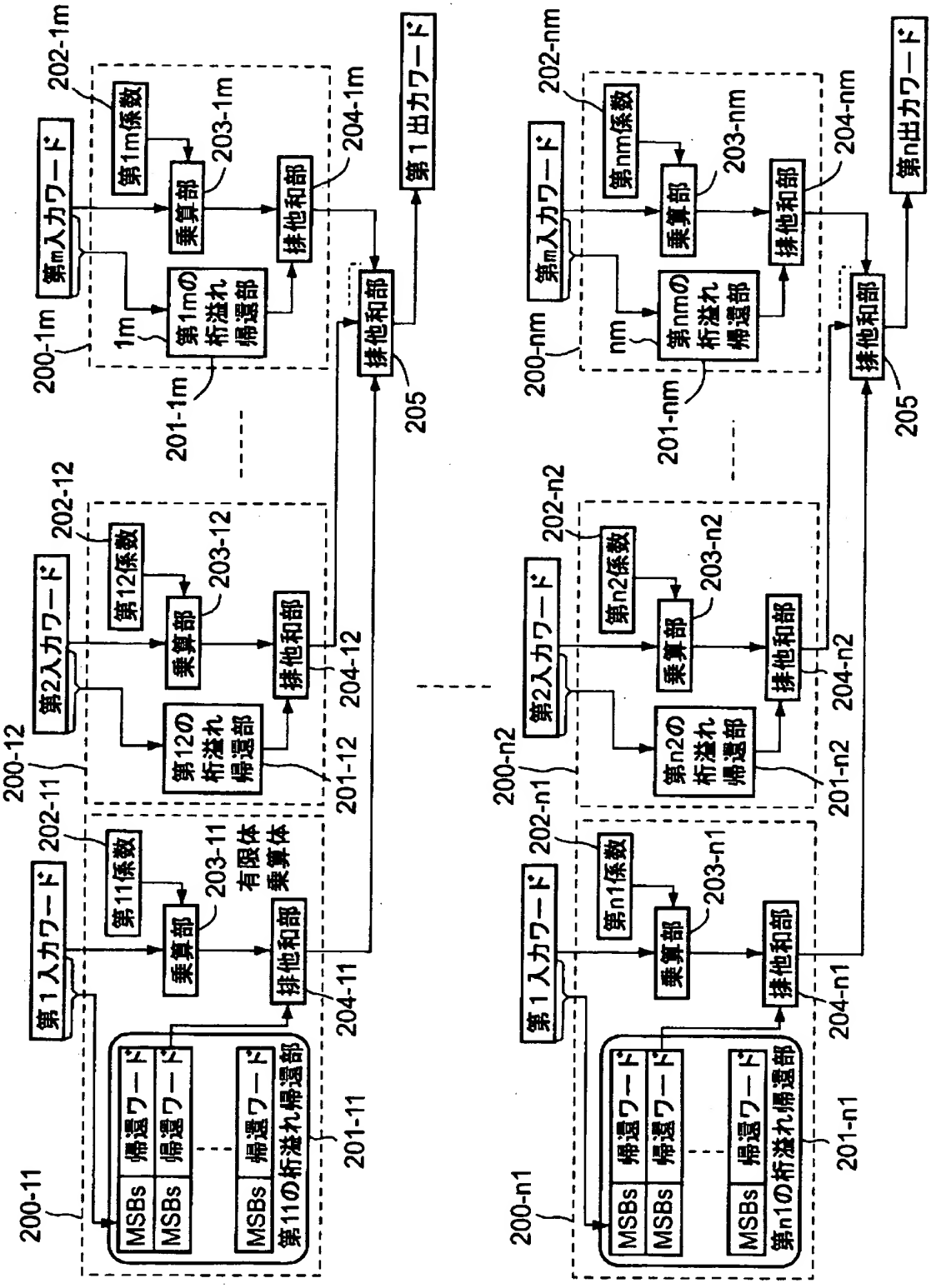
$$\begin{cases} H_0 = (5a827999)_H = 2^{1/2}/4 \\ H_1 = (6ed9eba1)_H = 3^{1/2}/4 \\ H_2 = (8f1bbcdc)_H = 5^{1/2}/4 \\ H_3 = (ca62c1d6)_H = 10^{1/2}/4 \end{cases}$$

【図１６】

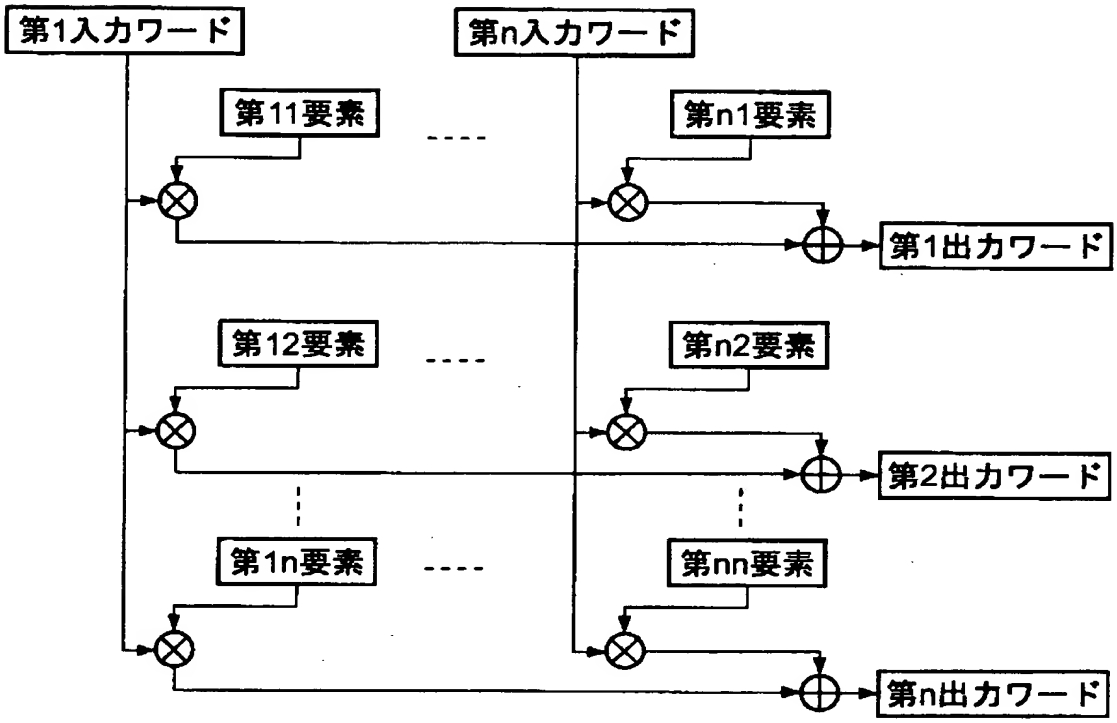


出証特２００１－３０５０９３８

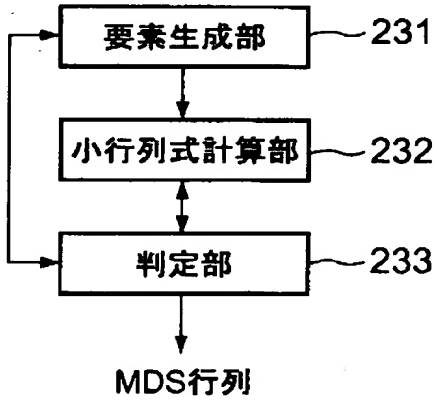
【図１７】


第1入力ワード
第2入力ワード
第mn入力ワード
第11係数
第12係数
第1m係数
第n1係数
第n2係数
第nm係数
乗算部
203-11
203-12
203-1m
203-n1
203-n2
203-nm
有限体乗算体
排他和部
204-11
204-12
204-1m
204-n1
204-n2
204-nm
205
第1出力ワード
第n出力ワード
MSBs
帰還ワード
第11の桁溢れ帰還部
第12の桁溢れ帰還部
第1mの桁溢れ帰還部
第n1の桁溢れ帰還部
第n2の桁溢れ帰還部
第nmの桁溢れ帰還部
200-11
200-12
200-1m
200-n1
200-n2
200-nm
201-11
201-12
201-1m
201-n1
201-n2
201-nm
202-11
202-12
202-1m
202-n1
202-n2
202-nm
1m
nm

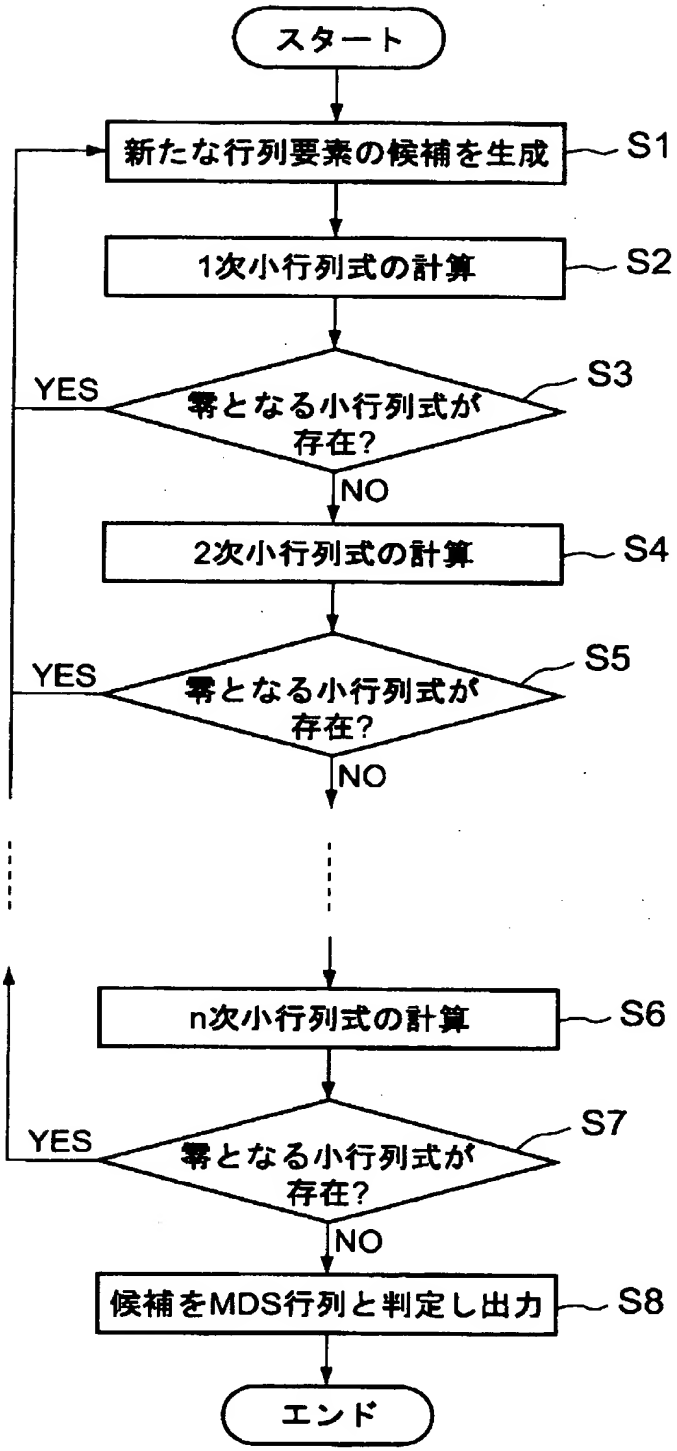
【図１８】


第1入力ワード
第n入力ワード
第11要素
第n1要素
第1出力ワード
第12要素
第n2要素
第2出力ワード
第1n要素
第nn要素
第n出力ワード

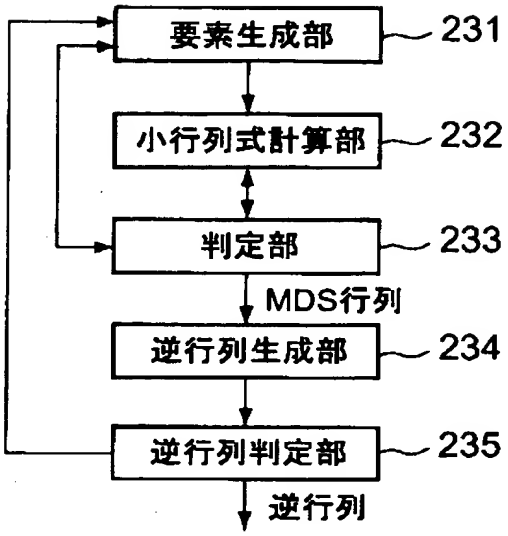
【図１９】


要素生成部
231
小行列式計算部
232
判定部
233
MDS行列

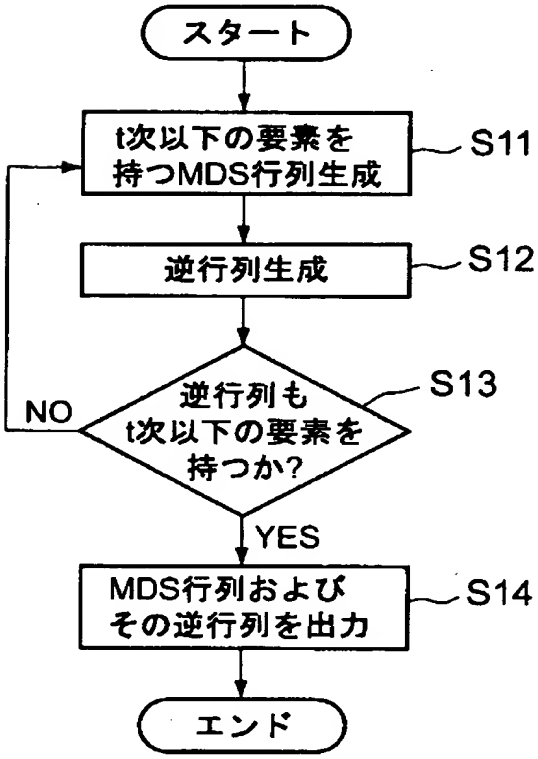
【図２０】


スタート
新たな行列要素の候補を生成
S1
1次小行列式の計算
S2
YES
零となる小行列式が存在?
S3
NO
2次小行列式の計算
S4
YES
零となる小行列式が存在?
S5
NO
n次小行列式の計算
S6
YES
零となる小行列式が存在?
S7
NO
候補をMDS行列と判定し出力
S8
エンド

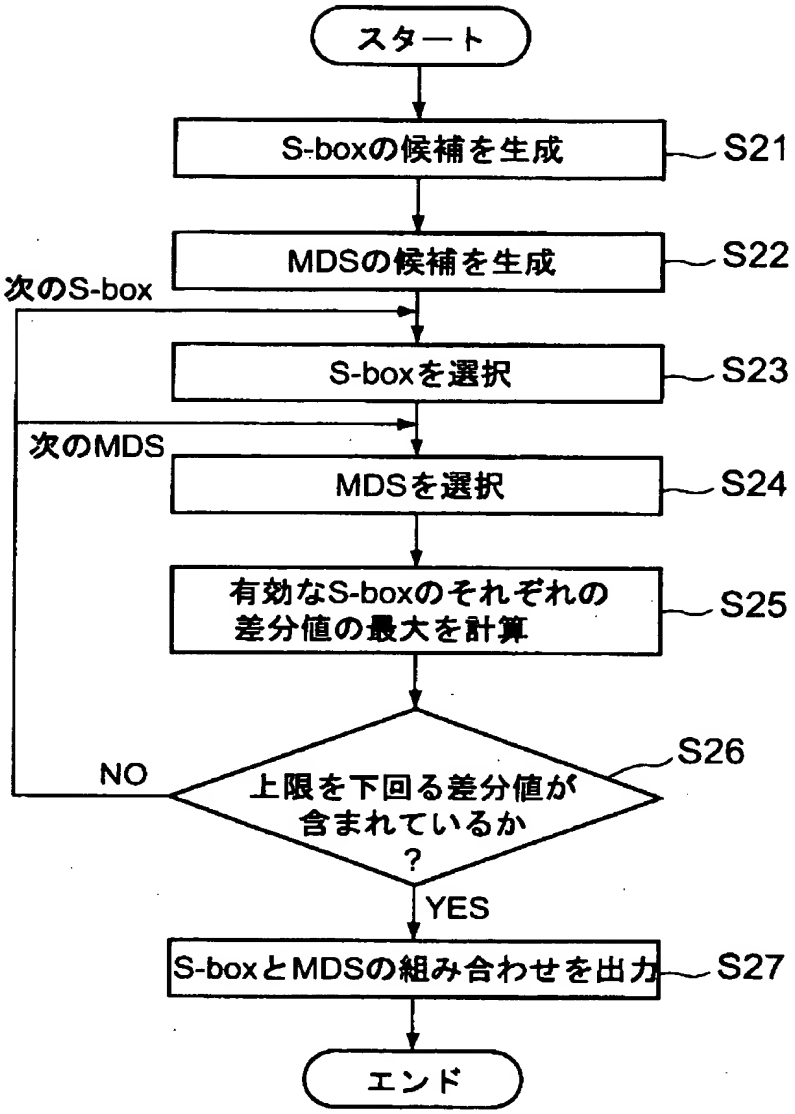
【図２１】


要素生成部
231
小行列式計算部
232
判定部
233
MDS行列
逆行列生成部
234
逆行列判定部
235
逆行列

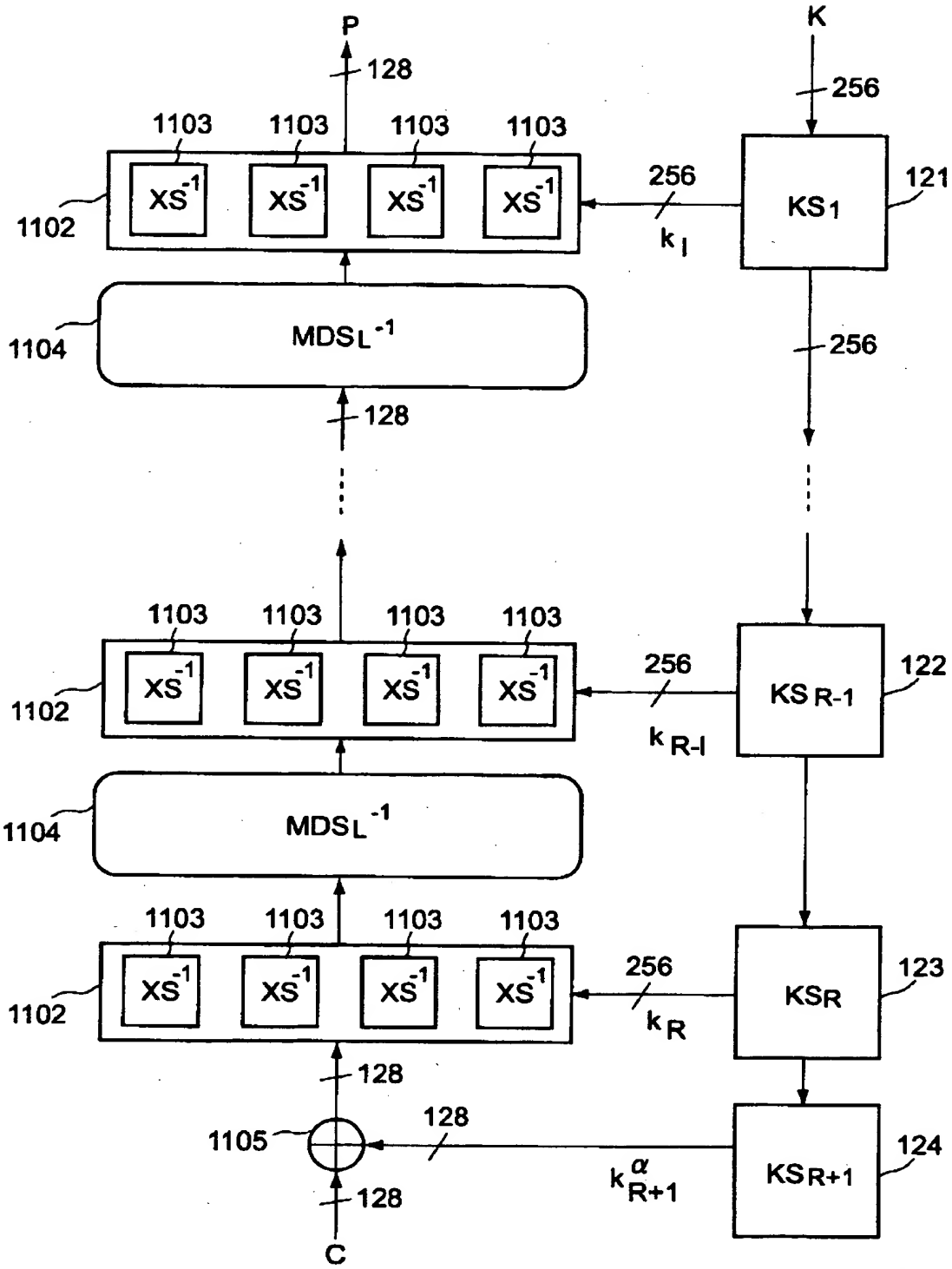
【図２２】


スタート
t次以下の要素を
持つMDS行列生成
S11
逆行列生成
S12
逆行列も
t次以下の要素を
持つか?
S13
NO
YES
MDS行列および
その逆行列を出力
S14
エンド

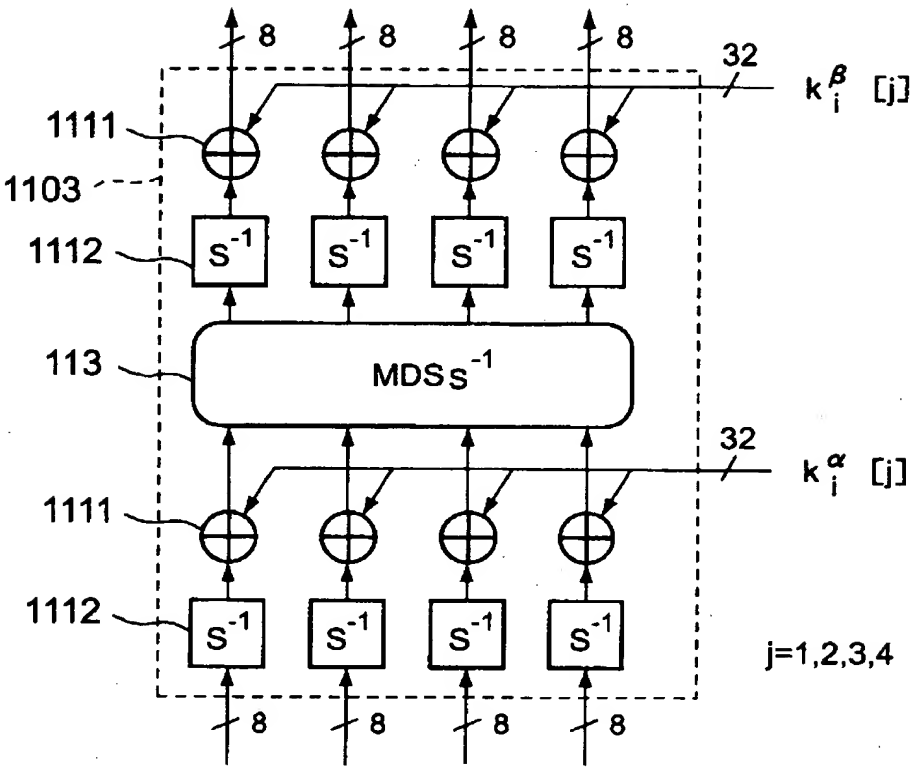
【図２３】


スタート
S-boxの候補を生成
S21
MDSの候補を生成
S22
次のS-box
S-boxを選択
S23
次のMDS
MDSを選択
S24
有効なS-boxのそれぞれの差分値の最大を計算
S25
NO
上限を下回る差分値が含まれているか？
S26
YES
S-boxとMDSの組み合わせを出力
S27
エンド

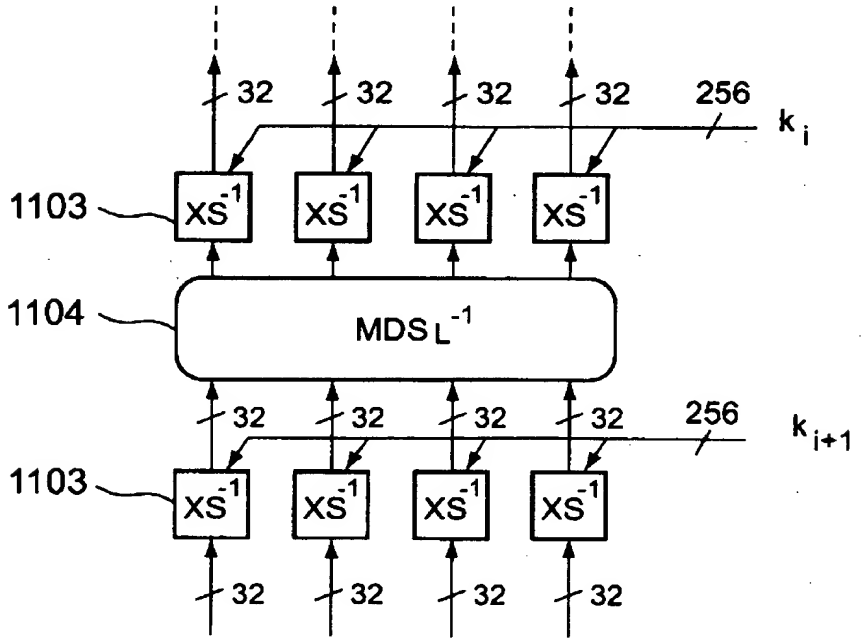
【図２４】


P
128
K
256
1103
1103
1103
1103
XS-1
XS-1
XS-1
XS-1
1102
256
k I
KS1
121
MDSL-1
1104
256
128
1103
1103
1103
1103
XS-1
XS-1
XS-1
XS-1
1102
256
k R-I
KS R-1
122
MDSL-1
1104
1103
1103
1103
1103
XS-1
XS-1
XS-1
XS-1
1102
256
k R
KSR
123
128
128
1105
k α R+1
KSR+1
124
128
C

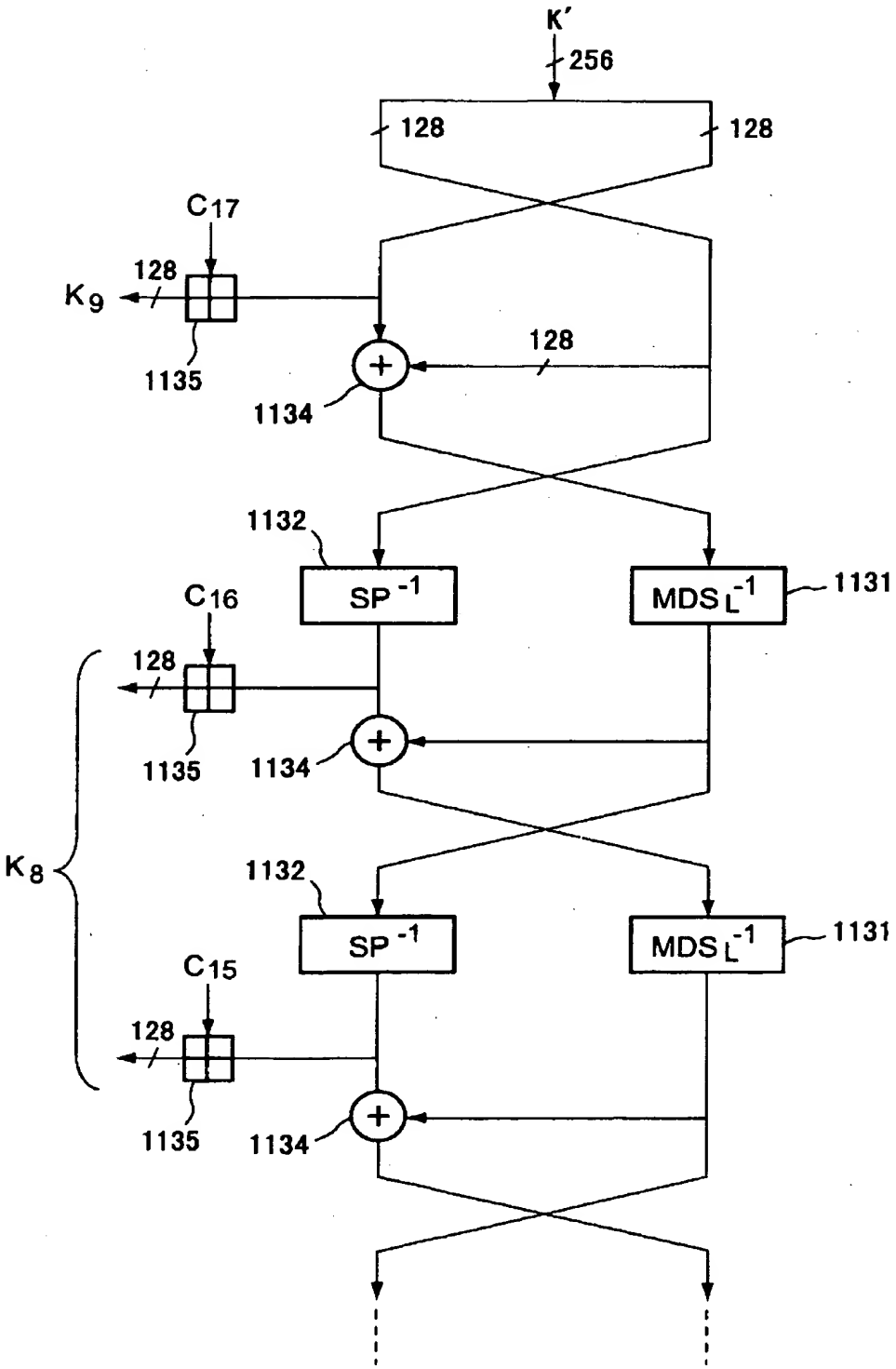
【図２５】


8
8
8
8
32
k_i^{β} [j]
1111
1103
1112
S^{-1}
113
$MDS S^{-1}$
32
k_i^{α} [j]
1111
1112
j=1,2,3,4

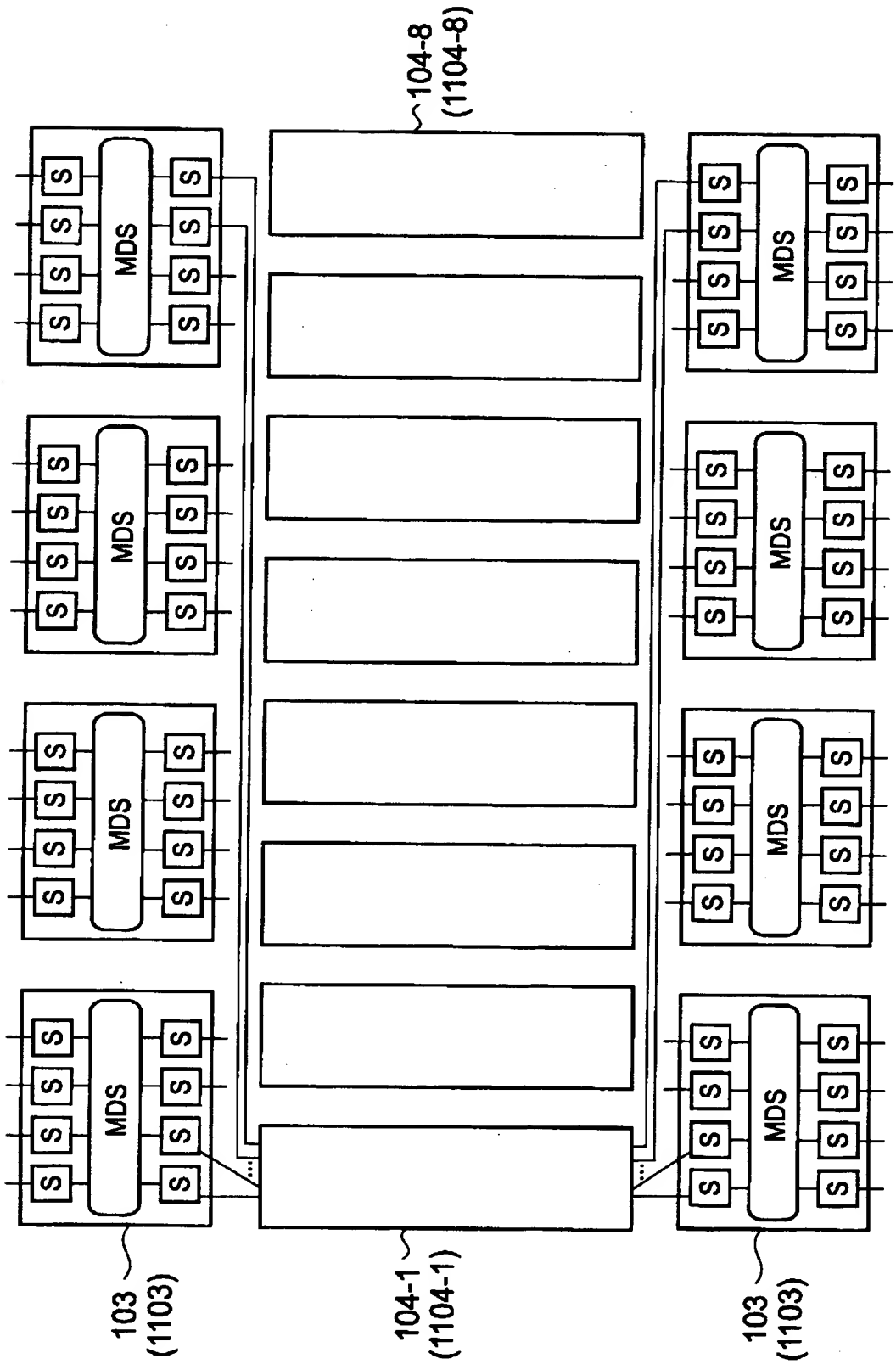
【図２６】


32
256
k_i
1103
XS^{-1}
1104
MDS_L^{-1}
k_{i+1}

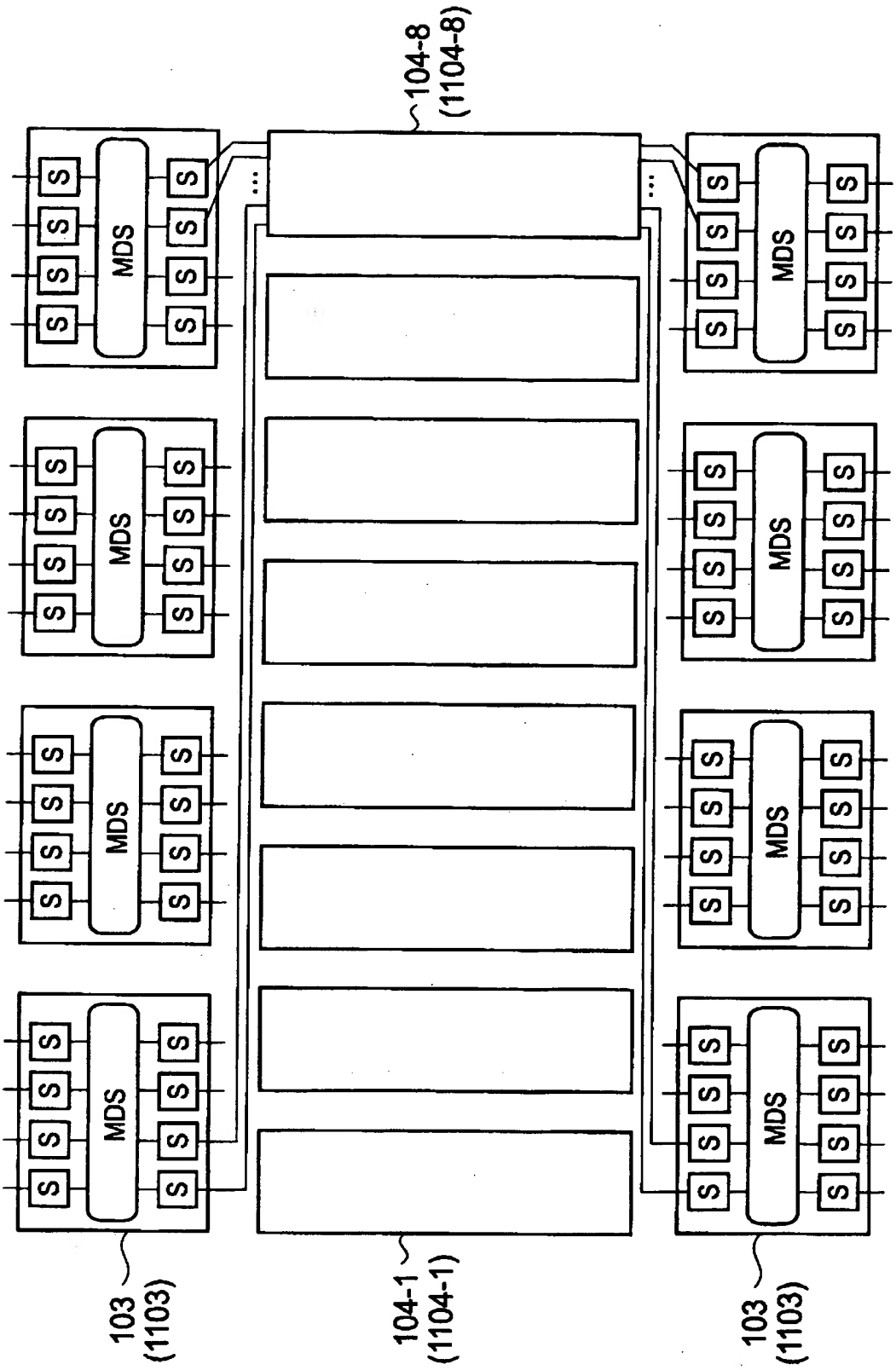
【図２７】


K'
256
128
128
C17
128
K9
1135
128
1134
1132
SP -1
MDS L -1
1131
C16
128
1135
1134
K8
1132
SP -1
MDS L -1
1131
C15
128
1135
1134

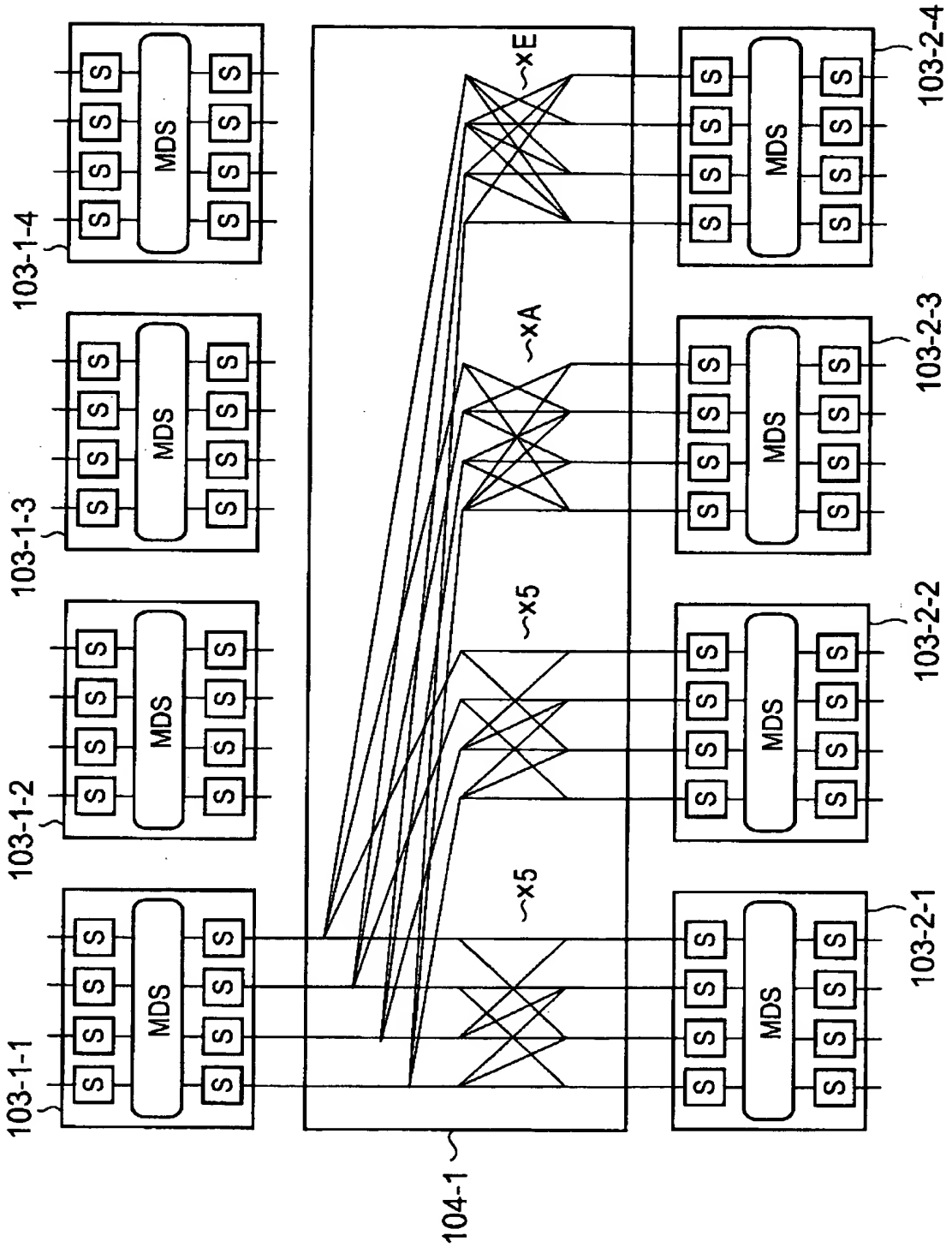
【図２８】



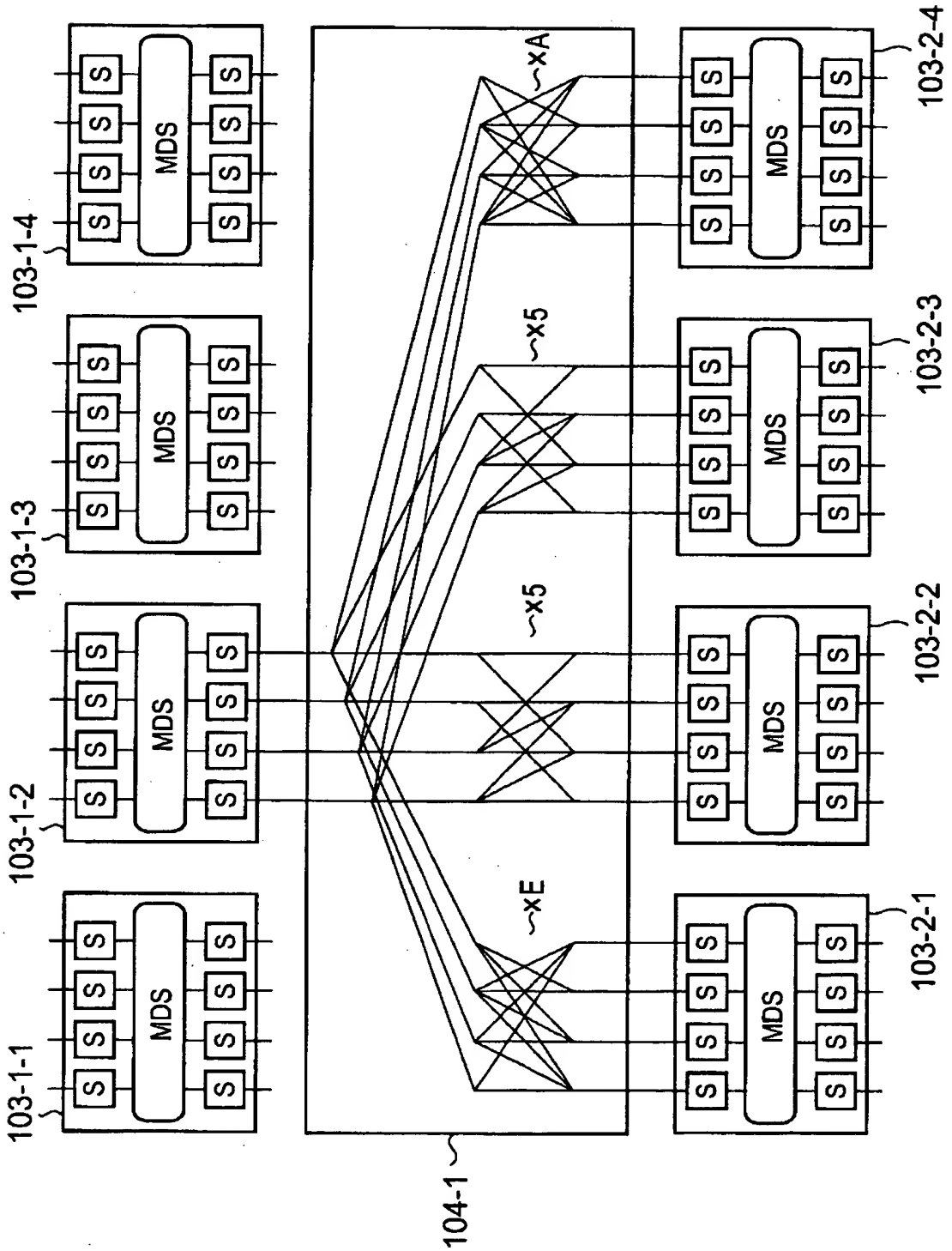
【図２９】



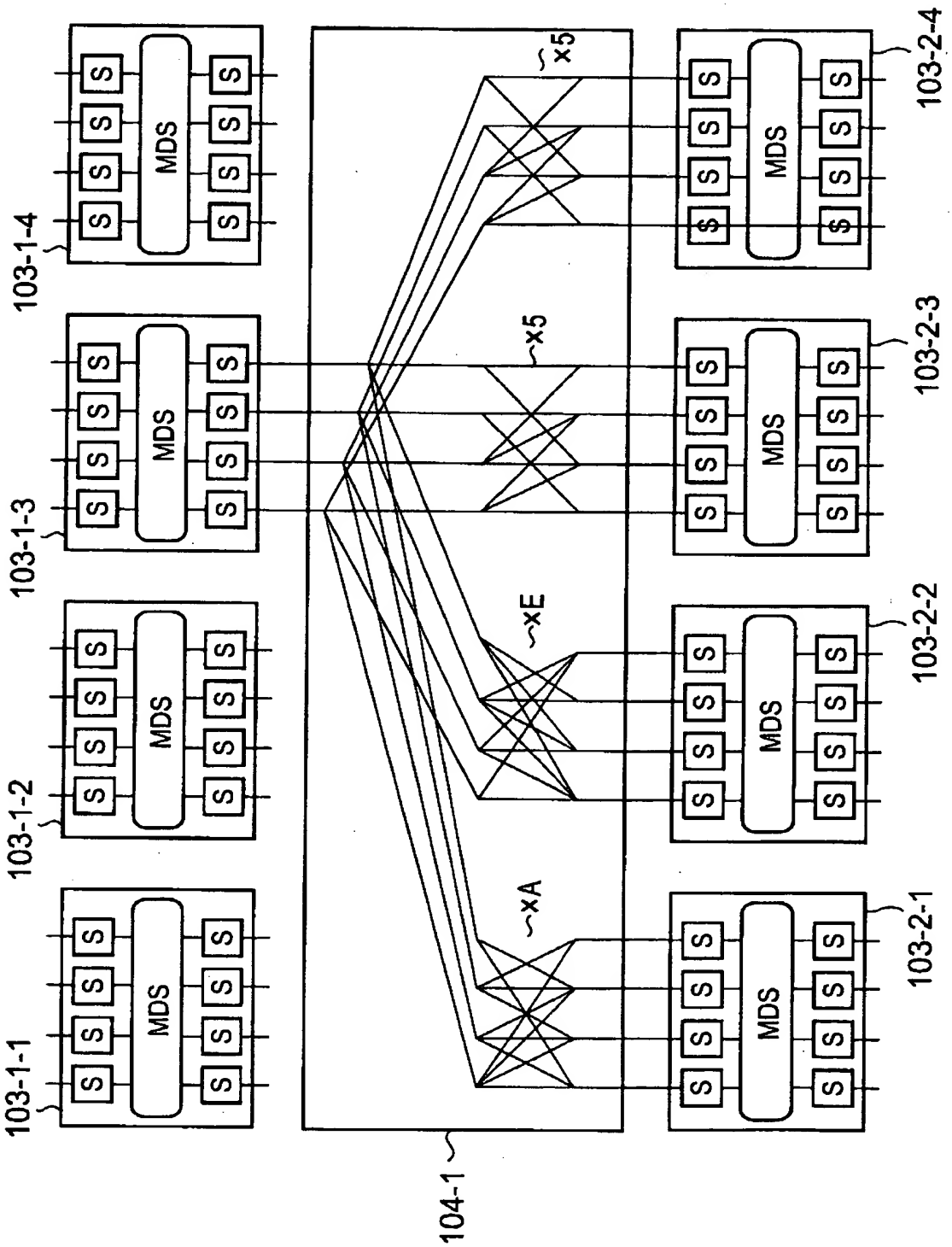
【図３０】


103-1-1
103-1-2
103-1-3
103-1-4
MDS
S
104-1
~x5
~x5
~xA
~xE
103-2-1
103-2-2
103-2-3
103-2-4

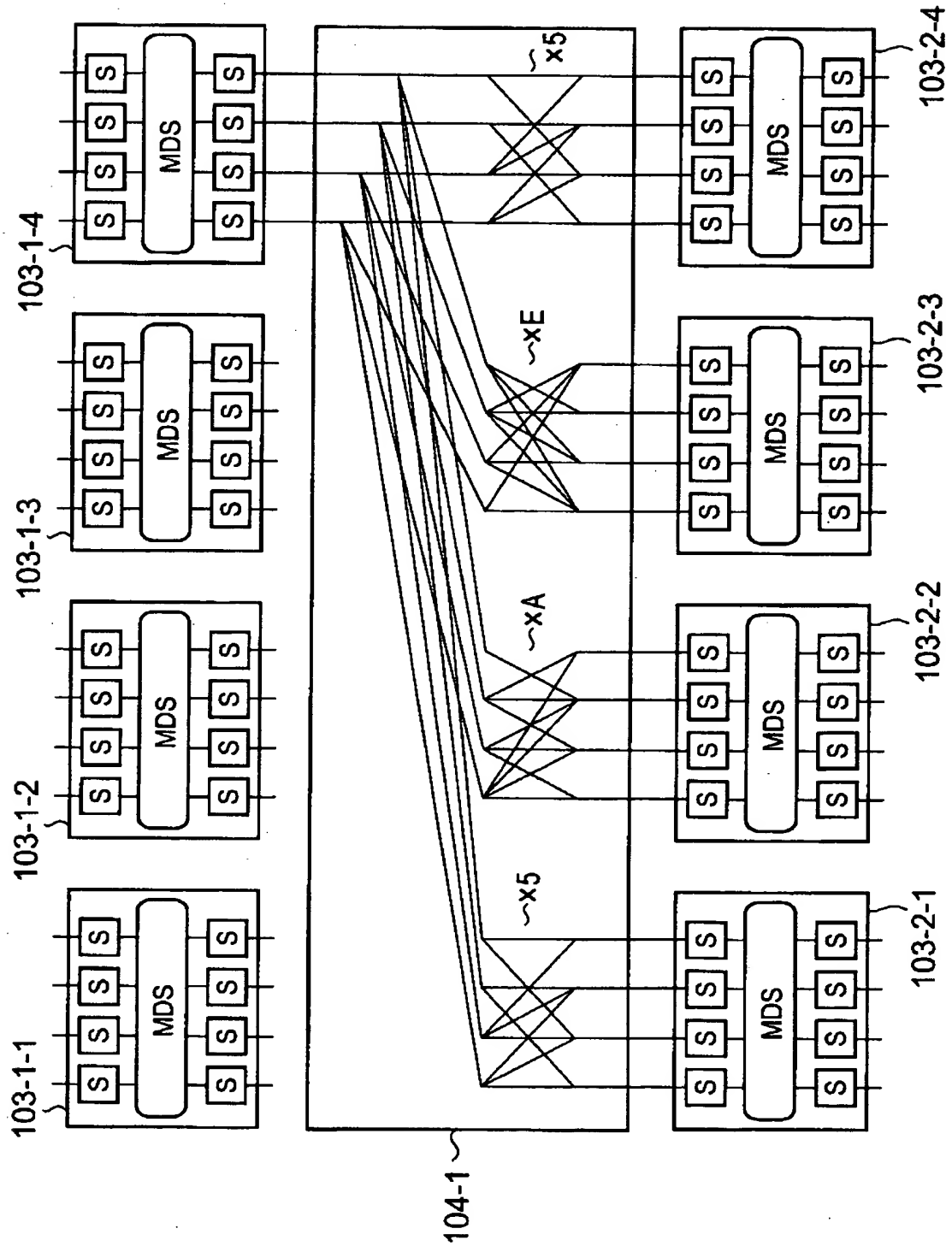
【図３１】


MDS
S
103-1-1
103-1-2
103-1-3
103-1-4
103-2-1
103-2-2
103-2-3
103-2-4
104-1
xA
x5
x5
xE

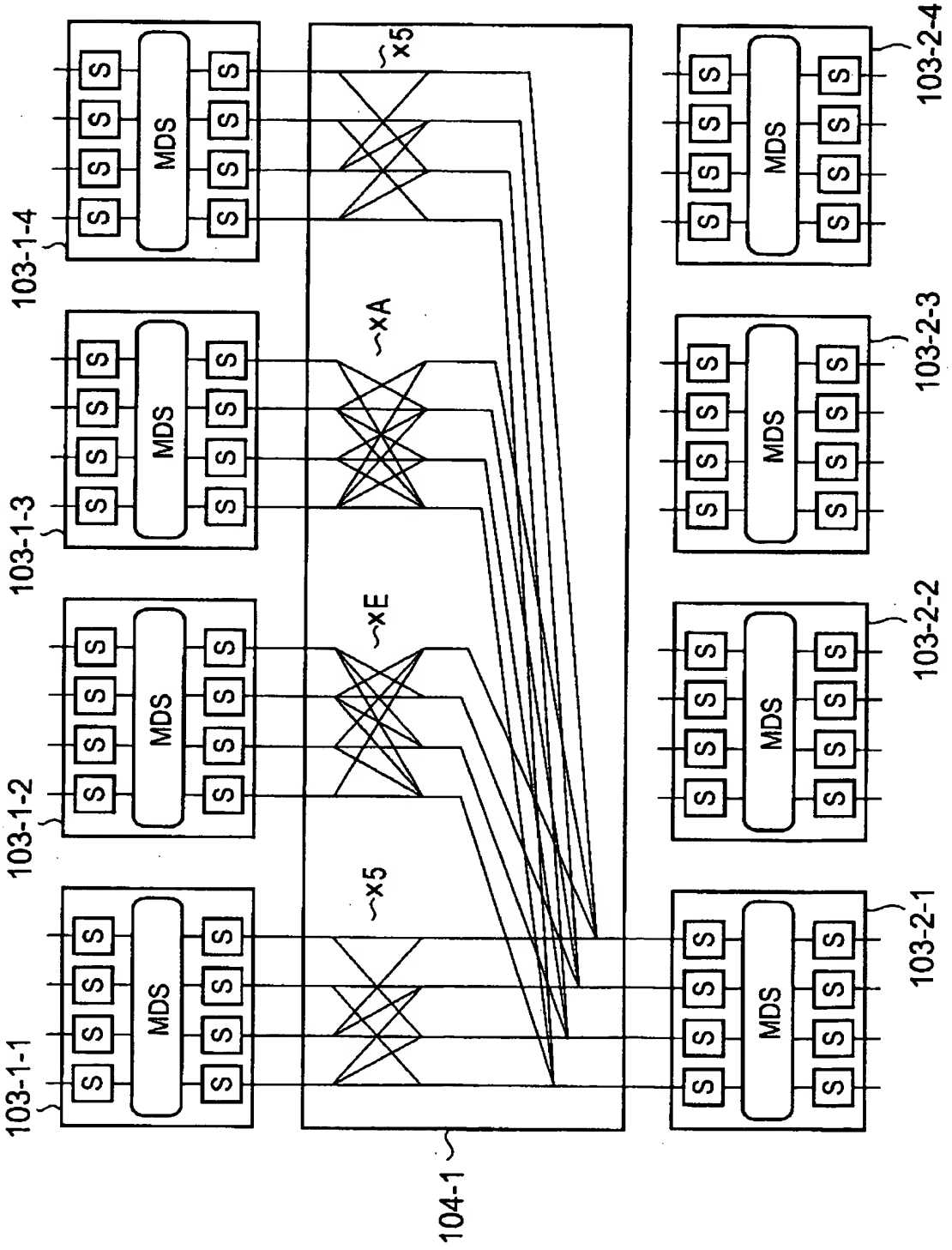
【図３２】


MDS
S
103-1-1
103-1-2
103-1-3
103-1-4
103-2-1
103-2-2
103-2-3
103-2-4
104-1
xA
xE
x5
x5

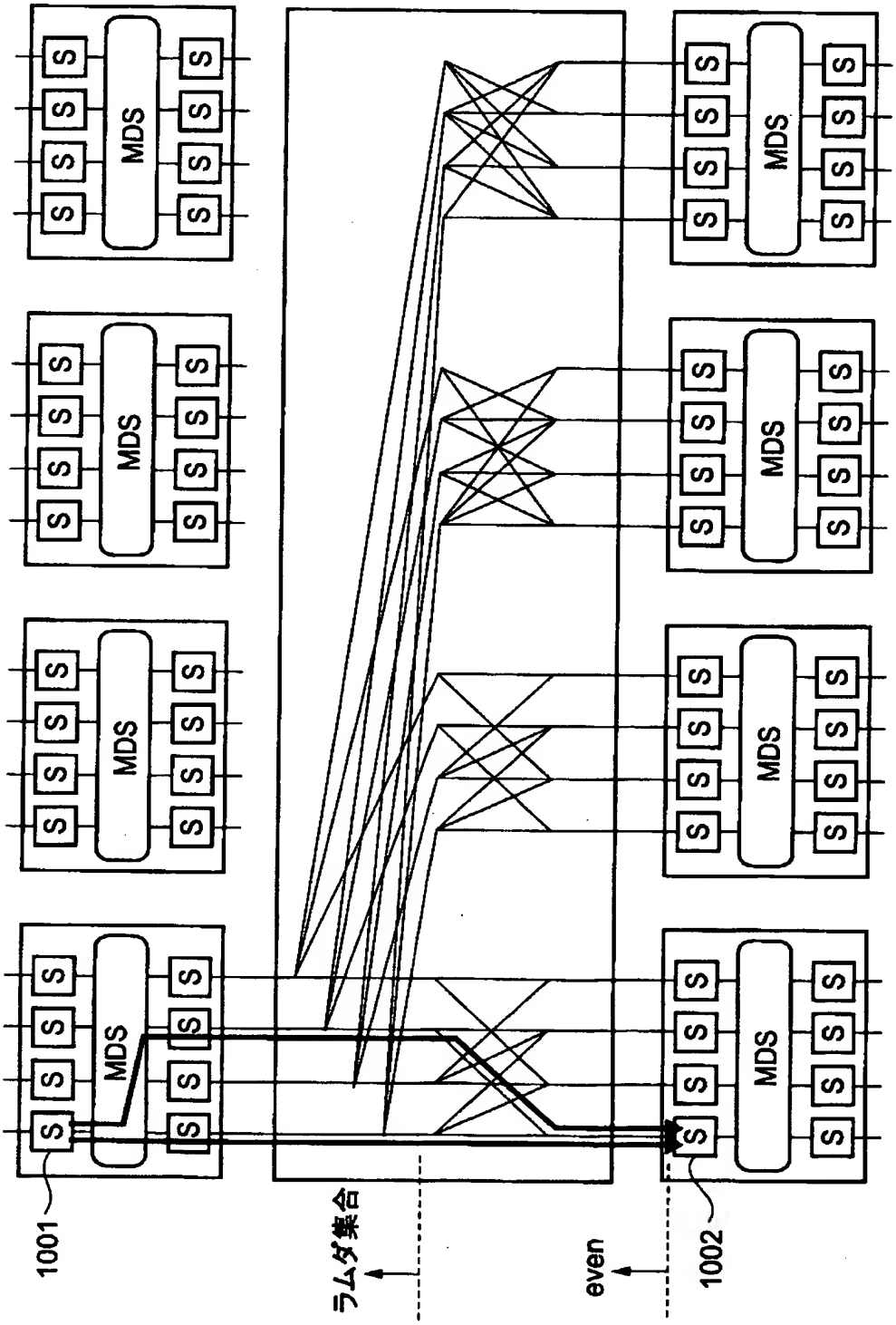
【図３３】


MDS
S
103-1-1
103-1-2
103-1-3
103-1-4
103-2-1
103-2-2
103-2-3
103-2-4
104-1
x5
xA
xE
x5

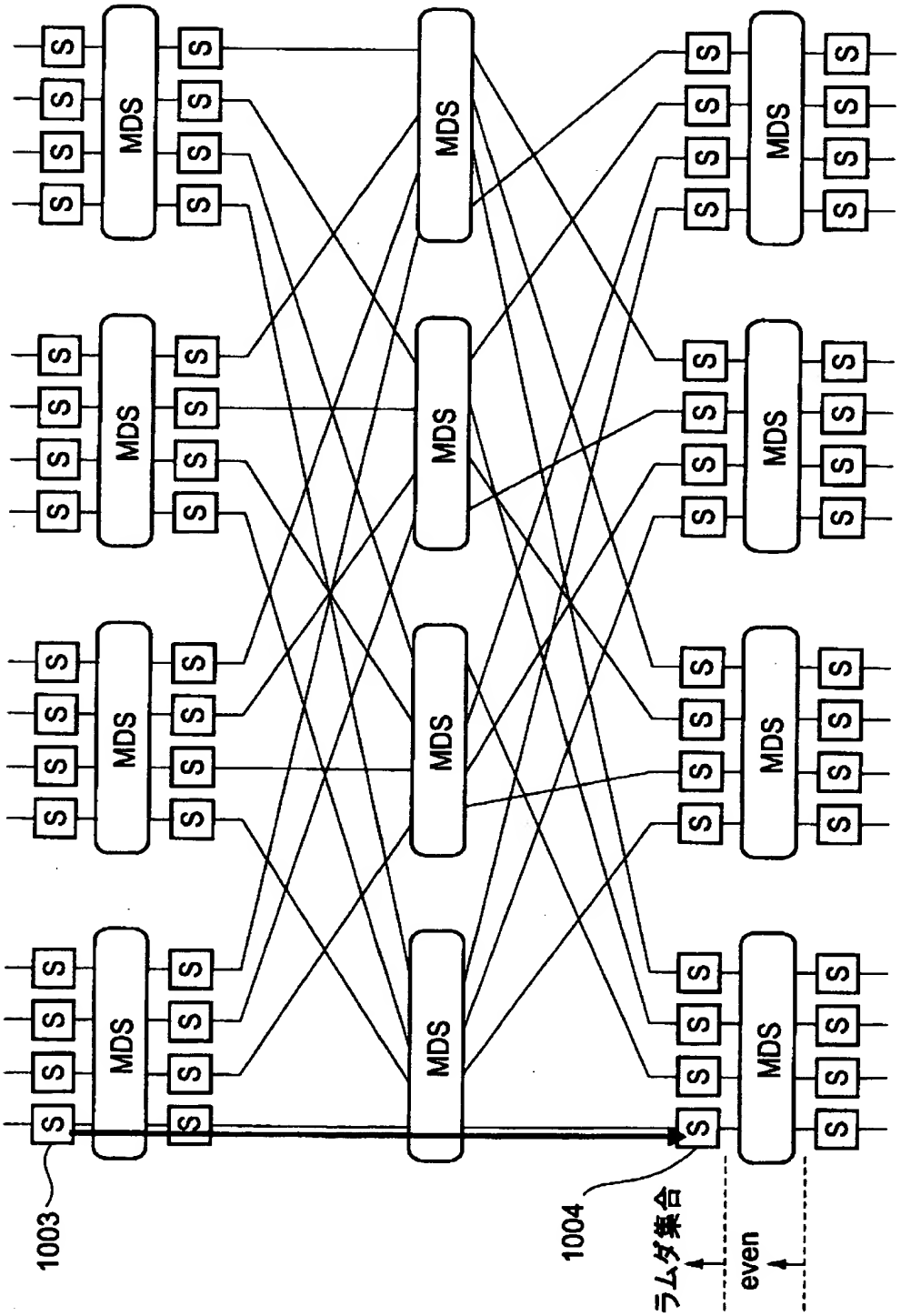
【図３４】


MDS
S
103-1-1
103-1-2
103-1-3
103-1-4
103-2-1
103-2-2
103-2-3
103-2-4
104-1
x5
xE
xA
x5

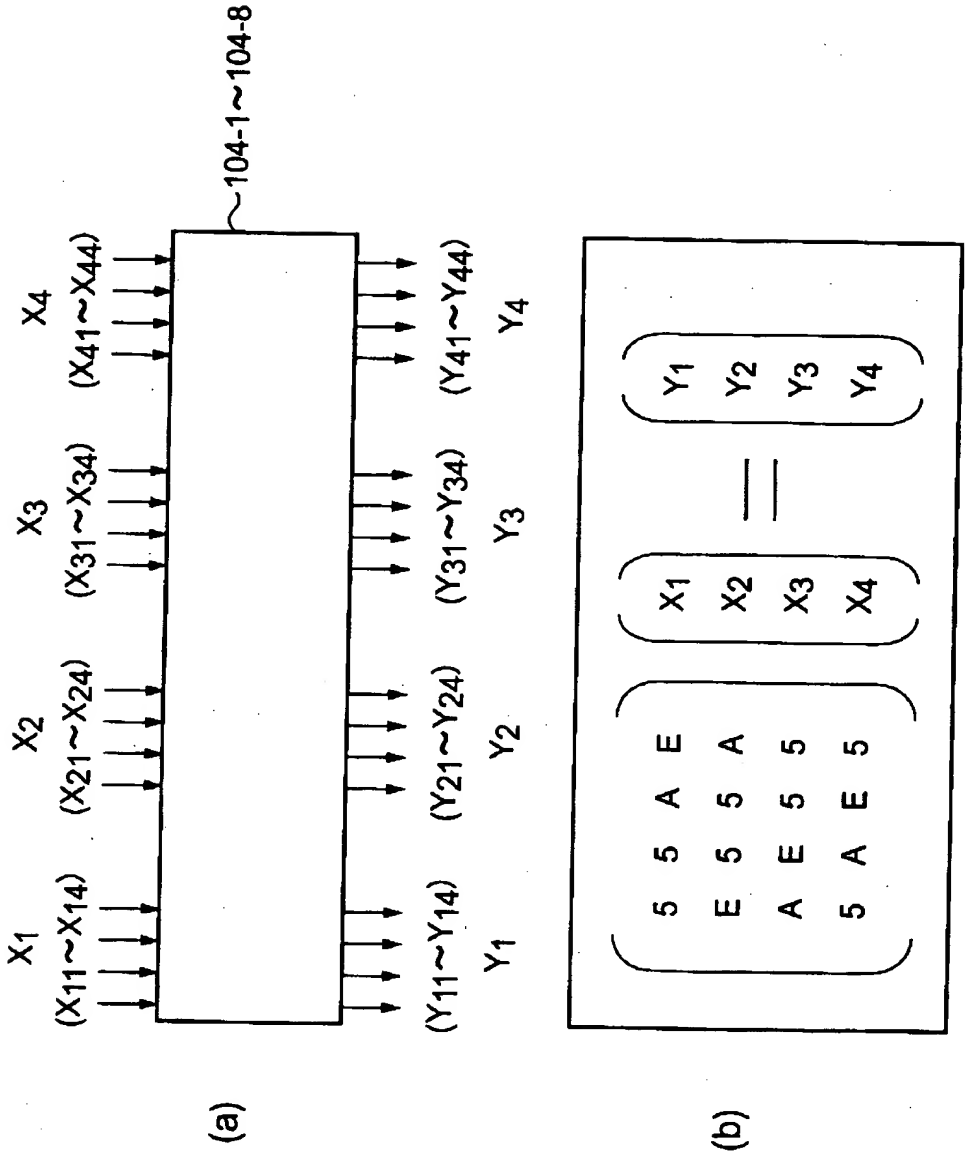
【図３５】



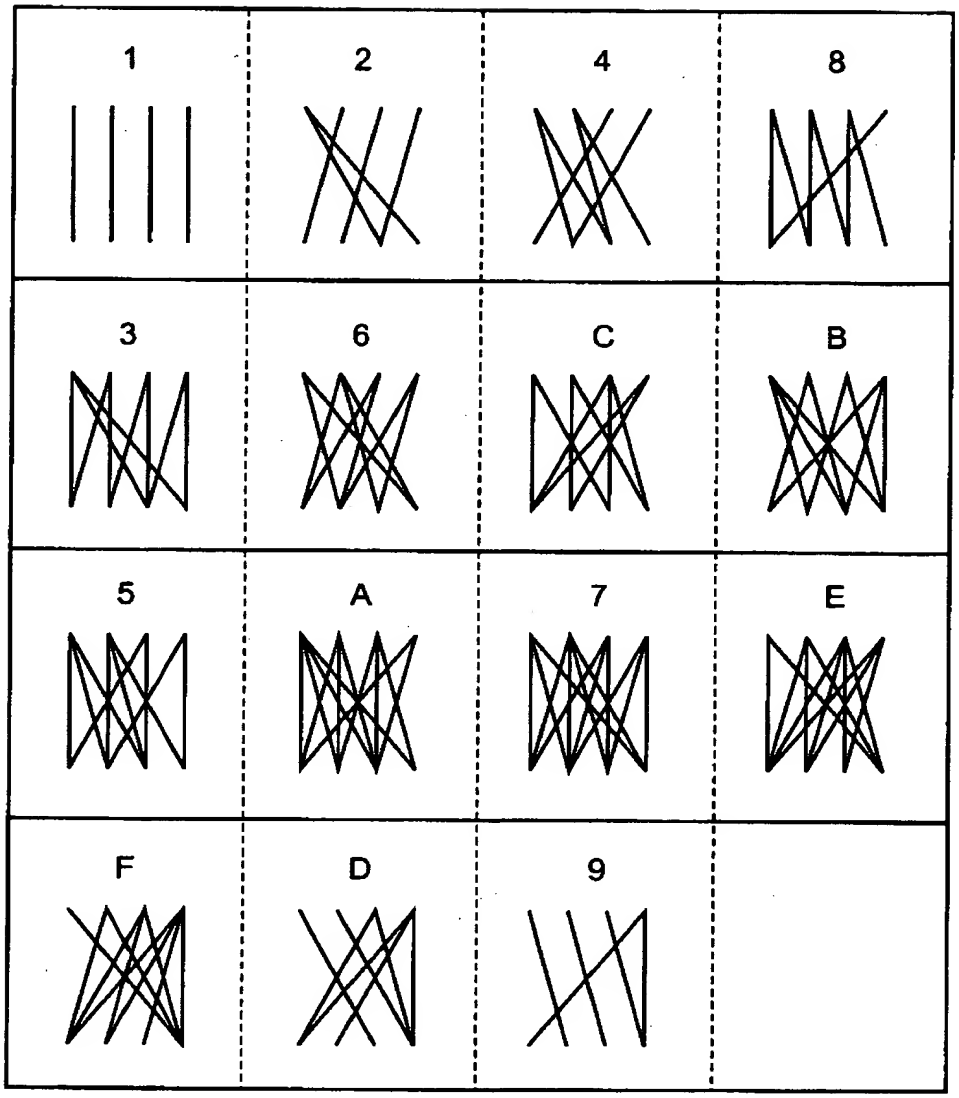
【図３６】



【図３７】


104-1～104-8
X1
(X11～X14)
X2
(X21～X24)
X3
(X31～X34)
X4
(X41～X44)
Y1
(Y11～Y14)
Y2
(Y21～Y24)
Y3
(Y31～Y34)
Y4
(Y41～Y44)
(a)
5 5 A E
E 5 5 A
A E 5 5
5 A E 5
X1 X2 X3 X4
Y1 Y2 Y3 Y4
(b)

【図３８】



【図３９】

(a)

$$\begin{pmatrix} 5 & 5 & A & E \\ E & 5 & 5 & A \\ A & E & 5 & 5 \\ 5 & A & E & 5 \end{pmatrix} = M_1$$

(b)

$$\begin{pmatrix} B & E & E & 6 \\ 6 & B & E & E \\ E & 6 & B & E \\ E & E & 6 & B \end{pmatrix} = M_2 = M_1^{-1}$$

(c)

$$\begin{pmatrix} 6 & B & E & E \\ E & 6 & B & E \\ E & E & 6 & B \\ B & E & E & 6 \end{pmatrix} = M_3$$

(d)

$$\begin{pmatrix} 5 & A & E & 5 \\ 5 & 5 & A & E \\ E & 5 & 5 & A \\ A & E & 5 & 5 \end{pmatrix} = M_4 = M_3^{-1}$$

【図４０】

(a)

$$\begin{pmatrix} 3 & 3 & 7 & C \\ C & 3 & 3 & 7 \\ 7 & C & 3 & 3 \\ 3 & 7 & C & 3 \end{pmatrix} = M_5$$

(b)

$$\begin{pmatrix} B & E & 3 & 3 \\ 3 & B & E & 3 \\ 3 & 3 & B & E \\ E & 3 & 3 & B \end{pmatrix} = M_6 = M_5^{-1}$$

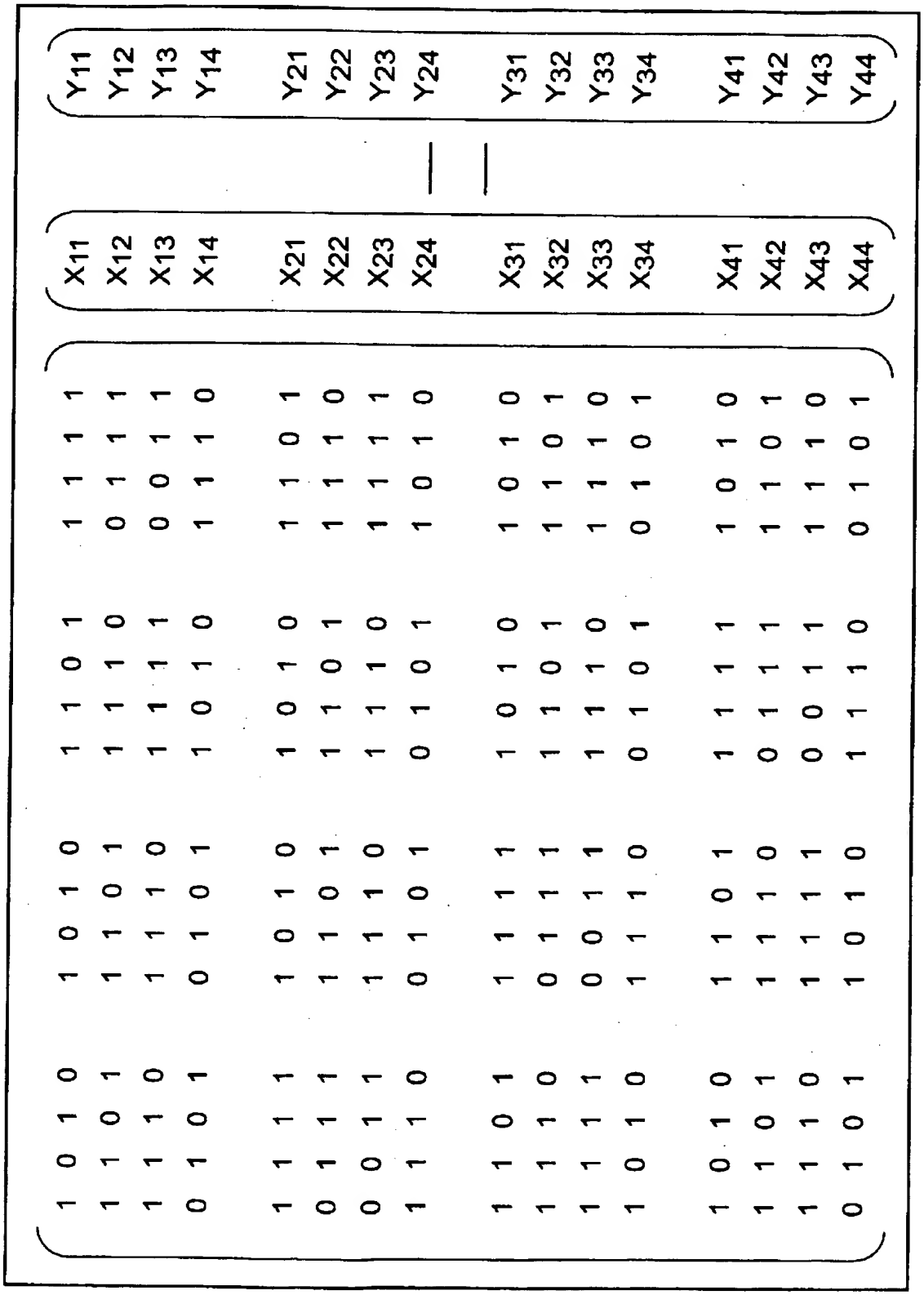
(c)

$$\begin{pmatrix} 3 & 3 & B & E \\ E & 3 & 3 & B \\ B & E & 3 & 3 \\ 3 & B & E & 3 \end{pmatrix} = M_7$$

(d)

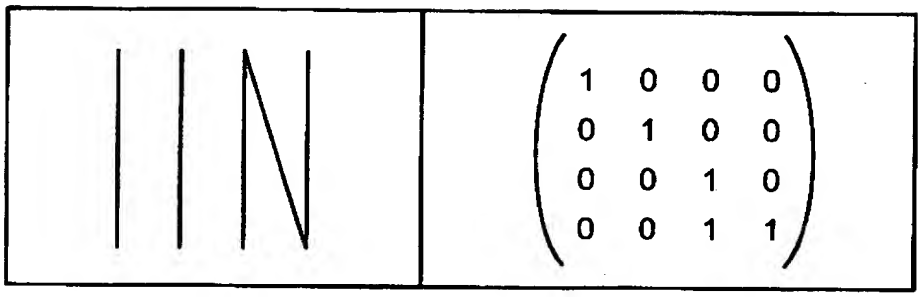
$$\begin{pmatrix} 7 & C & 3 & 3 \\ 3 & 7 & C & 3 \\ 3 & 3 & 7 & C \\ C & 3 & 3 & 7 \end{pmatrix} = M_8 = M_7^{-1}$$

【図４１】


Y11 Y12 Y13 Y14 Y21 Y22 Y23 Y24 Y31 Y32 Y33 Y34 Y41 Y42 Y43 Y44
X11 X12 X13 X14 X21 X22 X23 X24 X31 X32 X33 X34 X41 X42 X43 X44

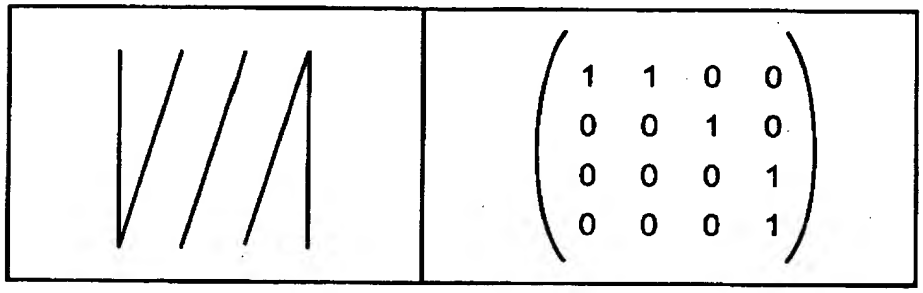
【図４２】

(a)



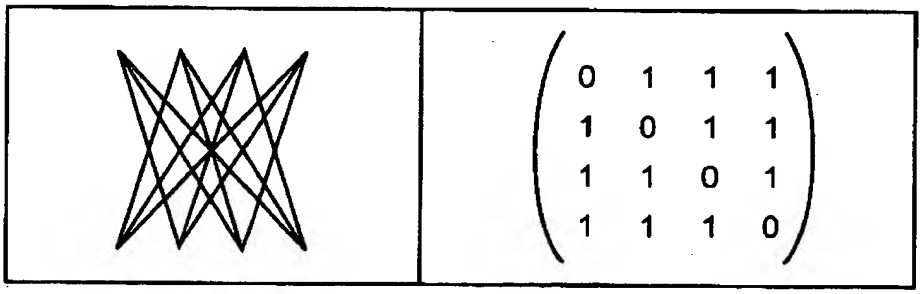
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

(a)



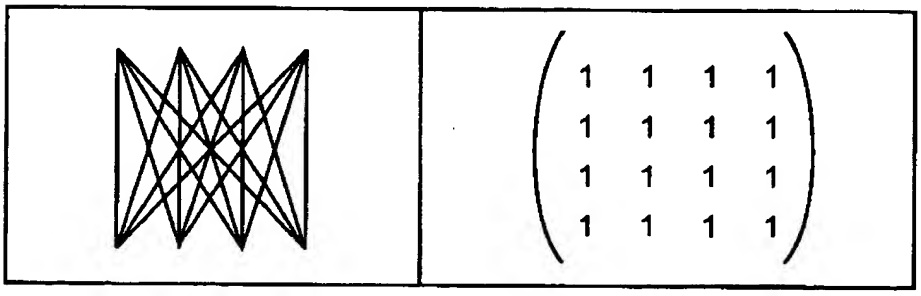
$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

(a)



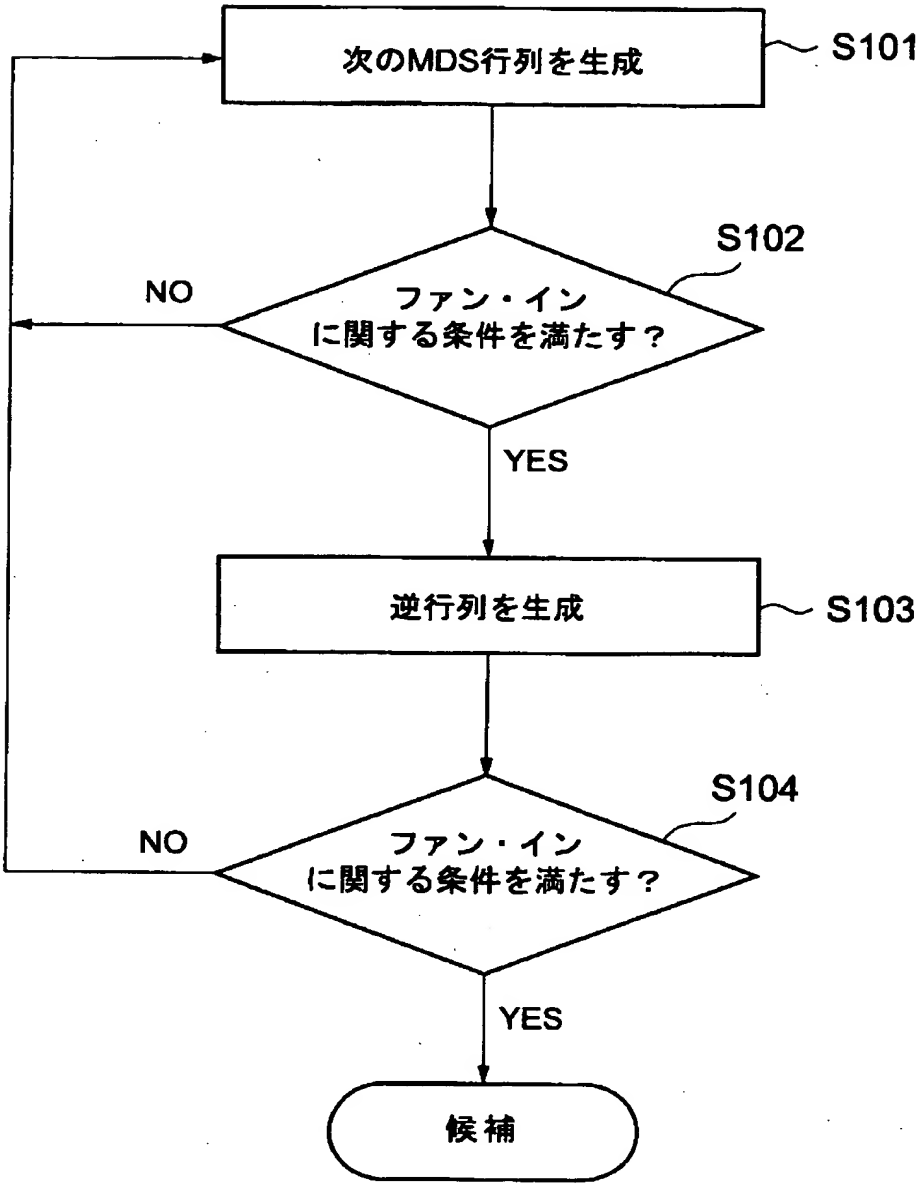
$$\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

(a)

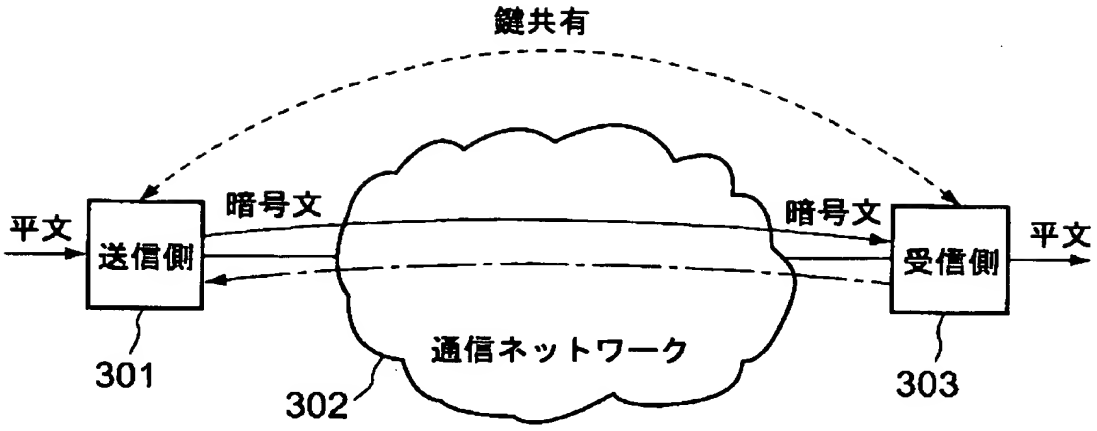


$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

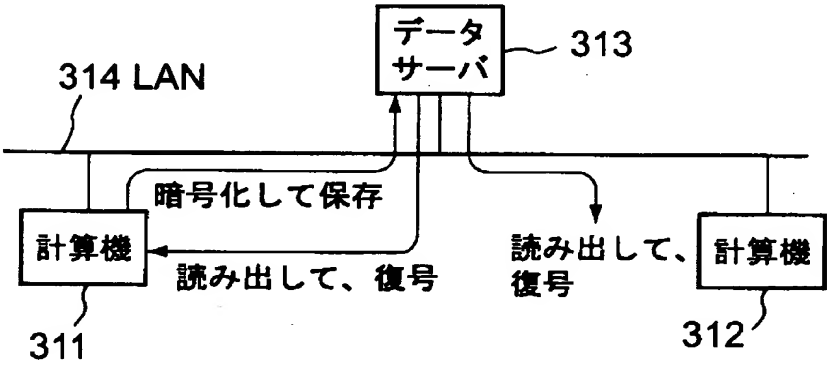
【図４３】


次のMDS行列を生成
S101
S102
ファン・イン
に関する条件を満たす？
NO
YES
逆行列を生成
S103
S104
ファン・イン
に関する条件を満たす？
NO
YES
候補

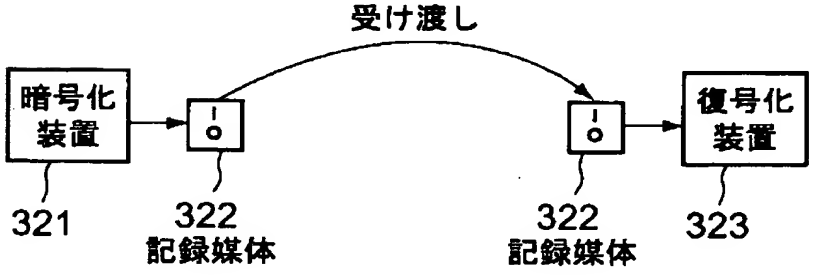
【図４４】


鍵共有
平文
送信側
暗号文
暗号文
受信側
平文
通信ネットワーク
301
302
303

【図４５】


データ
サーバ
313
314 LAN
暗号化して保存
計算機
読み出して、復号
読み出して、
復号
計算機
311
312

【図４６】


受け渡し
暗号化
装置
復号化
装置
321
322
記録媒体
322
記録媒体
323

【書類名】　　要約書

【要約】

【課題】　計算コストを抑えたまま高く均一な拡散を可能とする暗号化装置を提供すること。

【解決手段】　各段において複数並列に並んだ非線形変換モジュール２の各々により局所的な小拡散を行い、次いで拡散モジュール３によりブロック幅に渡る大拡散を行い、また非線形変換モジュール２により局所的な小拡散を行い、ということを所定段数繰り返す。さらに、非線形変換モジュール２は、非線形変換モジュール４と拡散モジュール５とを交互に配列して構成される。すなわち、入れ子型ＳＰＮ構造とする。拡散モジュール３は、前段の非線形変換モジュール群への入力データの少なくとも１つのビットの状態を後段の非線形変換モジュール群への入力データの少なくとも１つのビットへ複数の演算経路を辿って波及させるための線形変換を行う。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００３０７８〕

１．変更年月日　　１９９０年　８月２２日
［変更理由］　新規登録
住　所　神奈川県川崎市幸区堀川町７２番地
氏　名　株式会社東芝